



WikiLeaks Document Release

<http://wikileaks.org/wiki/CRS-RL33858>

February 2, 2009

Congressional Research Service

Report RL33858

*The Department of Homeland Security's Risk Assessment
Methodology: Evolution, Issues, and Options for Congress*

Todd Masse and Siobhan O'Neil, Domestic Social Policy Division; John Rollins, Foreign Affairs,
Defense, and Trade Division

February 2, 2007

Abstract. This report presents several risk assessment and related grant program options for congressional consideration: (1) maintain the status quo in the inextricably linked areas of risk assessment and grant allocation, (2) draft a national impact assessment to understand return on investment of the approximately \$12 billion of HSGP spent by FY2008, (3) enhance the transparency of the risk allocation methodology to state and local governments, and (4) develop a comprehensive and long-term strategy for managing, assessing and mitigating risk. To achieve these goals, the department could opt to consider procedural or organizational changes. Possible approaches are discussed in the report's final section.

WikiLeaks

CRS Report for Congress

The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress

February 2, 2007

Todd Masse
Specialist in Domestic Intelligence and Counterterrorism
Domestic Social Policy Division

Siobhan O'Neil
Analyst in Domestic Security and Intelligence
Domestic Social Policy Division

John Rollins
Specialist in Terrorism and International Crime
Foreign Affairs, Defense, and Trade Division

<http://wikileaks.org/wiki/CRS-RL33858>



Prepared for Members and
Committees of Congress

The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress

Summary

As early as his Senate confirmation hearing, Department of Homeland Security (DHS) Secretary Michael Chertoff advocated a risk-based approach to homeland security. Secretary Chertoff has stated "DHS must base its work on priorities driven by risk" and, increasingly, risk assessment and subsequent risk mitigation have influenced all of the department's efforts intended to enhance our nation's ability to prevent, respond to, and recover from future terrorist attacks and natural disasters. While the practice of risk analysis may be advanced in the insurance and financial industries, it is relatively less developed in the homeland security field. Although there are numerous reasons that account for this dynamic, two primary reasons include (1) the dynamic nature of terrorism and ability of terrorists to adapt to successful countermeasures, and (2) the lack of a rich historical database of terrorist attacks, which necessitates a reliance on intelligence and terrorist experts for probabilistic assessments of types of terrorist attacks against critical assets and/or regions. This report begins with an overview of the evolution of risk assessment methodologies from the Department of Justice in FY2002 to DHS in FY2007, and then discusses the discipline of risk management and risk assessment as applied to Homeland Security Grant Program (HSGP).

Terrorism risk analysis and assessment do not exist in a vacuum. Risk is analyzed and assessed as a means to mitigate or "buy down" risk over time by developing certain capabilities across the country. At DHS, the State Homeland Security Grant Program is the primary tool the agency has to influence the behavior of State and local partners to take actions that reduce what both parties agree are the risks of a terrorist attack and to respond effectively to such an attack, or other catastrophe. Regardless of the complexity of the risk assessment methodology, due to the inherent uncertainties associated with assessing risk in a dynamic counterterrorism context, some level of flexibility in managing risk may be necessary. Empirical data on historical terrorist attacks in the United States may, therefore, continue to play an important role in resource allocation to reduce risk.

This report presents several risk assessment and related grant program options for congressional consideration: (1) maintain the status quo in the inextricably linked areas of risk assessment and grant allocation, (2) draft a national impact assessment to understand return on investment of the approximately \$12 billion of HSGP spent by FY2008, (3) enhance the transparency of the risk allocation methodology to state and local governments, and (4) develop a comprehensive and long-term strategy for managing, assessing and mitigating risk. To achieve these goals, the department could opt to consider procedural or organizational changes. Possible approaches are discussed in the report's final section. This report may be updated.

Contents

Introduction	1
Background	2
Evolution of the DHS Risk Assessment Methodology	3
Risk Assessment-Related Legislative Activity	5
Risk Assessment: Stages of Development	5
Stage I: R=P	5
Stage II: R=T+CI+PD	5
Stage III: R=T*V*C=T*(V&C)	6
The Current Process	6
FY2007	6
The Current State	9
Transparency	9
Risk Formula Evolution	9
Guaranteed Minimums	9
Responsibility for Reducing Risk and Federal Grant Levels	10
Risk Assessment and Resource Allocation — Macro Questions	12
Risk Management and Assessment: Complex Activities	15
Risk Assessment: Some Critical Drivers and Perspectives	19
Possible Approaches for Congress	23
Maintaining Status Quo	23
National Impact Assessment	24
Further Enhance Transparency	24
Development of a Risk Strategy Both Within DHS and Throughout All Government Agencies	25
Appointment of a DHS Risk Assessment Manager (RAM)	26
Creation of a DHS Risk Advisory Board (RAB)	26
Creation of a Permanent Risk Assessment Center (RAC)	26
Implement 9/11 Commission Recommendation	27
Treat Terrorism Prevention Grants Uniquely	27
Appendix. Legislative Activity on DHS Risk Formula for Grants	29

List of Figures

Figure 1. Tracking Time Line	3
Figure 2. FY2007 Risk Formula	8
Figure 3. Asset-Based Risk Analysis Attributes	21
Figure 4. State Geographic Risk Analysis Attributes	21

List of Tables

Table 1. Evolution of DHS Grant and Risk Assessment Formula	11
---	----

The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress

Introduction

As early as his Senate confirmation hearing, Homeland Security Secretary Michael Chertoff advocated a risk-based approach to homeland security. Under Secretary Chertoff's direction, the use of risk assessment has become pervasive throughout DHS. Increasingly, risk assessment and subsequent risk mitigation efforts influence many aspects of the department's work intended to enhance our nation's ability to prevent, respond to, and recover from future terrorist attacks and natural disasters. Indeed, Secretary Chertoff has stated "DHS must base its work on priorities driven by risk."¹

The purpose of this report is to analyze how DHS assesses risk.² In the absence of sound risk assessment methods, the prioritization of homeland security activities at the federal, state, and local level is problematic. If DHS is to "prevent terrorist attacks within the United States,"³ one of its primary statutory missions, it needs to assess risk in an accurate manner. However, risk assessment does not occur in a vacuum; the end goal is to reduce and mitigate risk. All of DHS's employees work to reduce risk, respond to a terrorist attack or natural disaster should one occur, and/or protect the country by preventing dangerous materials or individuals from crossing U.S. borders. The primary tool DHS has to "buy down" or minimize risk and to influence the behavior of State and local public safety and law enforcement officials who collectively represent substantial "force multipliers" is the Homeland Security Grant Program. Others have written extensively about DHS grant programs and the allocation of such programs across the country.⁴

¹ U.S. Department of Homeland Security, "Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security," Press Release, July 13, 2005, Office of the Press Secretary, available at [http://www.dhs.gov/xnews/releases/press_release_0703.shtm], accessed Jan. 26, 2007.

² DHS is primarily concerned with assessment of terrorism risk. As a result, a terrorism risk assessment model is currently being used by the department to allocate resources for purposes which include, but also go beyond terrorism prevention, such as preparation and response to natural disasters.

³ See P.L. 107-296, Sec 101, codified at 6 U.S.C. §111.

⁴ A non-exhaustive list of these reports and articles includes CRS Report RL33583, *Homeland Security Grants, Evolution of Program Guidance and Grant Allocation Methods*, Aug. 7, 2006, by Shawn Reese; CRS Report RL33241, *FY2006 Homeland Security Grant* (continued...)

The purpose of this report is not to re-construct grant program research, but to examine the concept of DHS risk assessment itself and how the evolution of risk assessment flows through the DHS grant programs. The report has three sections (1) the evolution of risk assessment from the Department of Justice in FY2002 to DHS in FY2007, (2) fundamental questions about risk analysis as applied to homeland security, and (3) possible options for Congress. It will examine strategic questions about risk, and how risk is defined and distinguishable from other terms, such as vulnerability. Finally, the report will discuss a possible range of approaches for Congress with respect to DHS risk assessment practices, DHS's organization to assess risk, and the implementation of risk mitigation efforts using the DHS grant tool.

Given the focus of this report, an analysis of the DHS's risk assessment methodology through the lens of the homeland security grant process, some background information on the grant process is necessary. As previously stated, the risk assessment process cannot be examined in isolation. Rather, the context of the homeland security grant program is discussed to illuminate the homeland security risk assessment methodology and its implementation throughout various homeland security initiatives. This report may be updated.

Background

In FY2004, the allocation of homeland security grant monies inspired debate in states across the country. One often-reported anecdote noted that Wyoming's FY2004 State Homeland Security Grant Program (SHSG) award was \$14,360,000, while New York and California received \$78,827,000 and \$133,964,000, respectively.⁵ On its face, it seemed intuitive that New York and California would receive more money than Wyoming. But when examined in light of 2004 census bureau estimates, it appears that Wyoming received approximately \$28.34 in SHSG funding per capita while New York and California received \$4.10 and \$3.73 per capita, respectively.⁶ The rationale behind the disbursement of funds seemed counterintuitive to many, especially given the recent attacks and continued plots against locations in New York and California, to include the 1993 World Trade Center Bombing, the 1994 Blind Sheikh plot, the Millennium plot against Los

⁴ (...continued)

Distribution Formulas: Issues for the 109th Congress, Jan. 20, 2006, by Shawn Reese; The Heritage Foundation, *DHS 2.0: Rethinking the Department of Homeland Security*, Dec. 13, 2004, by James J. Carafano and David Heyman; Michael E. O'Hanlon et. al, The Brookings Institution, *Protecting the Homeland 2006/2007*; Michael E. O'Hanlon, "Homeland Security Funding: Urban Area Grant Maze," *Washington Times*, June 29, 2006; Council on Foreign Relations, *Backgrounder: Risk-Based Homeland Security Spending*, Feb. 8, 2006, by Eben Kaplan.

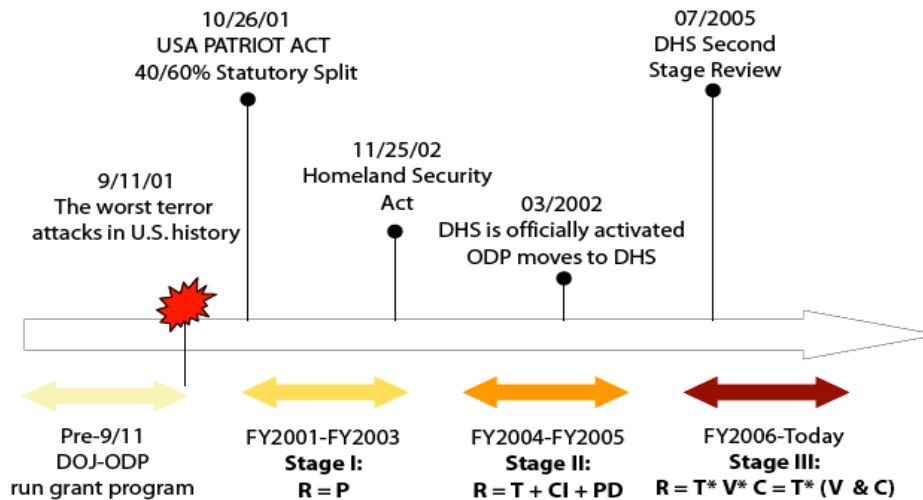
⁵ Department of Homeland Security, "FY2004 Homeland Security Grant Program," Department of Homeland Security Office of Grants and Training website, available at [http://www.dhs.gov], accessed on Dec.1, 2006, p. 7.

⁶ Comparison made using Department of Homeland Security's "FY 2004 Homeland Security Grant Program," and 2004 US population estimates from US census data.

Angeles International Airport (LAX), and the September 11th attacks, amongst others. Numerous interested stakeholders at all levels of government sought to learn more about the homeland security grant allocation methodology and process.

Figure 1 below provides a time line to track major milestone events in the evolution of risk assessment in a homeland security context.

Figure 1. Tracking Time Line



Source: CRS presentation of significant events and current law.

Risk experts appear to agree that all communities have some level of risk from terrorism. Yet, homeland security officials acknowledge that it is impossible to protect every target and harden every community to the extent that they become impervious to future attacks. It seems clear that it is necessary, from a national perspective, to identify the areas and entities across the country most at risk and to work to reduce that risk. What is less clear is the best way to evaluate *relative* homeland security risk, and establish an acceptable level of risk while attempting to close the most dramatic gaps between risk and capabilities. What follows is a chronological overview of the DHS risk assessment methodology examined through the prism of the Homeland Security Grant Program.

Evolution of the DHS Risk Assessment Methodology

The federal government's approach to distributing funds to State/local governments to enhance the latter's ability to prepare for and respond to terrorist acts has evolved in the last six years. It is important to understand the genesis of this grant program and the reactions to each stage of its development in order to better comprehend the current methodology. The evolution of the grant program and the risk methodologies it employs has occurred against the backdrop of the transformation of the nation's understanding of 'homeland security' itself. Borne out of the September 11 attacks, the term 'homeland security' and the department designed to enhance it, were initially solely terrorism-focused. With time, and other catastrophic incidents, the focus of the department expanded to include a range of

potentially destabilizing, non-terrorism threats, such as natural disasters. This evolution in mission has significant ramifications for the calculation of the threat aspect of the risk formulas utilized to allocate some of the homeland security grant funds, as will become evident in the following section's overview of grant allocation and related risk methodologies.

Over the years, there have been numerous criticisms from various groups⁷ over how risk is assessed and, as a result, DHS grants are allocated. Following the FY2004 homeland security grant allocation process, the 9/11 Commission (hereafter Commission) weighed in on the funding controversy when it issued the following recommendation in its final report, published in late July 2004:

Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Now, in 2004, Washington, D.C., and New York City are certainly at the top of any such list. We understand the contention that every state and city needs to have some minimum infrastructure for emergency response. But federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support. Congress should not use this money as a pork barrel.⁸

The Commission report asks a second question: "Can useful criteria to measure risk and vulnerability be developed that assess all the many variables?"⁹ The Commission lists a variety of factors that should be considered in the assessment of "threats and vulnerabilities" to include "population, population density, vulnerability, and the presence of critical infrastructure within each state."¹⁰ The Commission suggests that the federal government should then require each State that receives such funds to provide an "analysis based on the same criteria to justify the distribution of

⁷ For the past several grant cycles, many States and local leaders have expressed frustration and disappointment with DHS's risk assessment process and the related distribution of grant funds. Much of the disappointment with respect to FY2006 grants was the result of the first post-9/11 decline in funds provided to state and local communities. For FY2006, the total amount allocated for homeland security grants was \$1.7 billion, (DHS, "DHS Announces \$1.7 Billion in Homeland Security Grants: Grants will build States' and Urban Areas' Preparedness," May 31, 2006) a significant decrease from \$2.5 billion in FY2005 (DHS, "Homeland Security Grants FY2005," Updated December 3, 2004, Office of Grants and Training). Another source of frustration was a perceived lack of transparency regarding the risk assessment process, especially with regard to the sources of information used and the weighting of the formula's variables and underlying data sub-elements. Furthermore, the continued shift towards a risk-based approach may have caused consternation amongst some jurisdictions due to the inference that future grant funding may be threatened. Spurred on by congressional pressure, the department has continued to move toward a methodology that is more heavily risk-based.

⁸ National Commission of Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, Authorized Edition (New York: WW Norton and Company, 2004), p. 396.

⁹ Ibid.

¹⁰ Ibid.

funds [with]in that State.”¹¹ The Commission understood that the “benchmarks” chosen to evaluate a site’s threat and vulnerability “...will be imperfect and subjective; [but] they will continually evolve.”¹²

Given the criticisms associated with the DHS risk assessment methods, a look at congressional interest in risk assessment as it relates to the homeland security grant programs may be instructive.

Risk Assessment-Related Legislative Activity¹³

Concurrent with the Commission’s critique and internal efforts within DHS to move to a more risk-based approach, Members of Congress put forth a series of bills and amendments to the Homeland Security Act that sought to reform the criteria for distributing homeland security grant funds. Each effort sought to remedy the perceived issues associated with the homeland security risk assessment process. Some suggested the creation of new oversight or coordination bodies. Most importantly, for purposes of this report, each bill and amendment proposed changes to reduce guaranteed allotments and enhance the percentage of funding allocated based on risk. To varying detail, each legislative initiative suggested definitions or approaches to evaluate risk with regards to homeland security. The **Appendix** provides additional information on the legislative initiatives referenced in this section.

Understanding the criticisms of the DHS risk assessment process and the proposed congressional remedies, an analysis of how the various stages of risk assessment have evolved over time may be useful.

Risk Assessment: Stages of Development

There have been at least three stages in the evolution of risk assessment methodology as it pertains to homeland security. These stages and unique developments within each era are summarized below.

Stage I: R=P. This period covers from FY2001, when the Department of Justice (DOJ) had primary responsibility for assessing risk, to FY2002-FY2003, when this responsibility was transferred to DHS. This first stage of risk assessment could be characterized as early stage developmental. During this period, risk was generally assessed and measured according to population numbers. In short, risk (R) was equated to population (P).

¹¹ Ibid.

¹² Ibid.

¹³ The intent of this section and the appendix is to provide a snapshot of recent historical and current legislative activity with respect to risk assessment. This section is not provided with intent to track this legislation over time and, as such, will not be continually updated.

Stage II: $R=T+CI+PD$. This period covers from FY2004 to FY2005. During this period, the importance of critical infrastructure, population density¹⁴ and a number of other variables was included in the assessment of risk. However, the formula for risk remained additive and “risk-like,” as probabilities were not an essential element of the risk assessment process. Risk was assessed as the sum of threat (T), critical infrastructure (CI), and population density (PD).

Stage III: $R=T*V*C=T*(V\&C)$. This period covers from FY2006 to today, a time when probability of particular events was systematically introduced into the formula. As will be discussed more in-depth below, FY2006 also marked another important departure from the previous risk assessment methodology: For the first time, when calculating risk, DHS chose to examine both risk to assets and geographic areas. With the swearing in of Michael Chertoff as Secretary of the DHS in February 2005, the department underwent both organizational and strategy-related changes. Concurrent with DHS’s reorganization, Secretary Chertoff announced that a new risk-based methodology would dictate departmental activities and all future federal funds would be distributed accordingly.¹⁵ This new approach to allocating the remaining funds required an assessment of risk using a formula that considers the threat to a target/area, multiplied by vulnerability (V) of the target/area, multiplied by consequence (C) of an attack on that target/area. As a result, the risk assessment formula became $R=T*V*C$. Variables were no longer additive, but were multiplied, implying weighting of variables and some assessment of the likelihood that certain events would occur.

The Current Process

FY2007. The FY2007 Homeland Security Grant Guidance describes the DHS approach to risk assessment as:

Risk will be evaluated at the Federal level using a risk analysis model developed by DHS in conjunction with other Federal entities. Risk is defined as the product of three principal variables:

- **Threat (T)** — the likelihood of an attack occurring

¹⁴ It should be noted that population density numbers can be misleading. Cities define geographic boundaries differently which may lead to municipalities with similar populations having very different density ratios. While population density is often a good indicator of individuals that may be affected by a terrorist attack, such a criteria may not be useful for cities where the citizens are located far away from the center of the municipality.

¹⁵ Secretary Michael Chertoff U.S. Department of Homeland Security Second Stage Review Remarks, July 13, 2005, available at [http://www.dhs.gov/xnews/speeches/speech_0255.shtm], accessed Jan. 26, 2007. “We must make tough choices about how to invest finite human and financial capital to attain the optimal state of preparedness. To do this we will focus preparedness on objective measures of risk and performance. Our risk analysis is based on these three variables: threat, vulnerability, and consequences. These variables are not equal. For example, some infrastructure is quite vulnerable, but the consequences of an attack are relatively small; other infrastructure may be much less vulnerable, but the consequences of a successful attack are very high, even catastrophic.”

- **Vulnerability and Consequence (V&C)** — the relative exposure and expected impact of an attack¹⁶

Although DHS continues to discuss its risk methodology in terms of the $R=T*V*C$ formula, it appears as if the department is treating vulnerability (V) and consequence (C) as an amalgamated, single variable as depicted in **Figure 2**. As mentioned above, due to difficulties associated with differentiating vulnerability values across areas and states, according to DHS it has, in effect, assigned a value of one to vulnerability. As a result, while three variables may formally remain in the formula, in effect only two exist for FY2007. In addition, significant changes to the underlying elements of each variable were made for the FY2007 process.¹⁷

While the FY2007 HSGP Guidance¹⁸ does not provide additional detail as to the specifics of the risk methodology, a separate document, the FY2007 DHS *Grant Programs Overview*, accompanying the Guidance sent to state homeland security leaders does provide greater transparency into how risk is assessed. In the *FY2007 DHS Grant Programs Overview*, the weighting of each variable is provided and includes a description of the underlying data-sets supporting the calculation for each variable. As demonstrated in **Figure 2** the vulnerability¹⁹ and consequence variables of the risk methodology now include the sub-elements of population index (comprising 40% of the risk methodology), a national infrastructure index (15%), an economic index (20%), and a nation security index (5%).

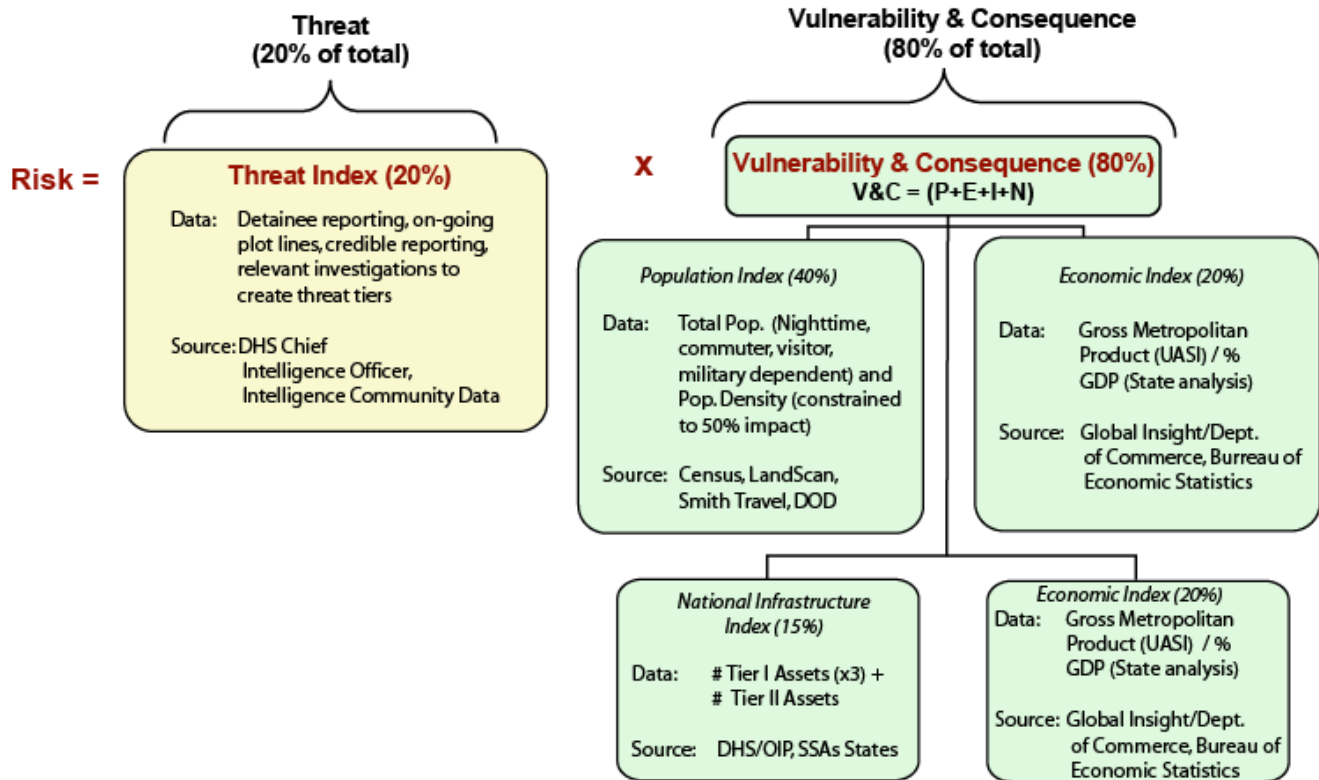
¹⁶ U.S. Department of Homeland Security, “FY2007 Homeland Security Grant Program: Program Guidance and Application Kit,” Office of Grants and Training website, available at [http://www.ojp.usdoj.gov/odp/docs/fy07_hsgp_guidance.pdf], p.8, accessed Jan. 29, 2007.

¹⁷ Though not the focus of the report, it is important to demonstrate how the evolution of the risk methodology has supported the significant changes included in the FY2007 Guidance. Two significant changes are contained in the FY2007 Guidance directly related to DHS’s risk methodology evolution: the dividing of the Urban Area Security Initiative jurisdictions into two tiers with the six municipalities in tier one receiving 55% of the total allocation and the department’s establishment of a pilot program to allow the six highest risk UASI cities authorized to use up to 25% of the awarded funds to support the personnel costs associated with counterterrorism operations.

¹⁸ U.S. Department of Homeland Security, FY2007 Homeland Security Grant Program, Program Guidance and Application Kit, Office of Grants and Training website, available at [http://www.ojp.usdoj.gov/odp/docs/fy07_hsgp_guidance.pdf], accessed Jan. 29, 2007.

¹⁹ As mentioned above, for FY2007, vulnerability has been assigned a value of one. In effect, then, consequence is weighted at 80%.

Figure 2. FY2007 Risk Formula



Source: CRS presentation of DHS FY2007 Risk Formula.

In FY2007, DHS's manner for determining threat (20% of the risk methodology) underwent a significant change in how intelligence and investigative information was analyzed. DHS's Office of Intelligence and Analysis for the first time undertook an historical analysis of threats to the representative UASI cities that spanned from the attacks of September 11, 2001, to the release of the FY2007 Homeland Security Grant Guidance. Prior to FY2007, in supporting the Homeland Security Grant effort, DHS evaluated threats to cities for the preceding year only and did not consider historical threat trends. For FY2007, DHS also initiated an effort whereby the cities deemed most at risk were placed in four tiers based on assessed level of threat.

It should be noted that DHS's efforts to evaluate and analyze threats only consider federal government intelligence and investigative information. To date, State and local intelligence and investigative information are not systematically considered in DHS's assessment of threats to a given locality. It could be argued that the establishment of the State and local fusion centers may assist in ensuring relevant

State and local threat information²⁰ is considered in future federal government risk analysis efforts.

The Current State. The evolution of the DHS risk assessment process and formula, as summarized in **Table 1**, continues to spark additional questions and some concerns in the following areas: the transparency of the risk assessment process; the implications of an evolving risk formula; minimum grant allotments; and the responsibility for buying down risk.

Transparency. The additional information provided by the department in FY2007 should allow applicants of DHS grant funds to have a better understanding of the types of information contained in the underlying data-sets and how each is assessed and weighted during the risk assessment process. While this transparency in the methodology may satisfy some grant process critics, others remain concerned with the formula's effectiveness in meeting the needs of those most at risk.²¹

Risk Formula Evolution. With the adoption of $R=T*V*C$, many see FY2006 as the first significant change to DHS's risk assessment methodology. Some observers could express concern that continued changes to the methodology will not allow the United States to establish a baseline of risks to the nation, thus jeopardizing any attempts to spot current trends or forecast future security concerns. Others might view the changes to the methodology as steps toward improving the risk assessment process and suggest that as DHS's understanding of risk evolves and its access to data increases, the associated methodology will stabilize and provide a sound foundation from which to make analytic and grant decisions.

Guaranteed Minimums. Some homeland security observers suggest that future congressional or executive branch changes to DHS's risk-based formula

²⁰ It has recently been reported that "...homeland security officials are opposed to letting representatives of State and local governments serve on..." the Interagency Threat Assessment Coordination Group (ITACG). See Siobhan Gorman, "Out of the Loop on Terror Threats: Homeland Security Excludes, State, Local Officials from Group that Shares Data," *Baltimore Sun*, Feb. 2, 2007. The ITACG was recommended in the *Information Sharing Environment (ISE) Implementation Plan*, published in Nov. 2006, by the Program Manager of the Information Sharing Environment, a group located within the Office of the Director of National Intelligence. According to the *ISE Implementation Plan* (p.29), "...A primary purpose of the ITACG will be to ensure that classified and unclassified intelligence produced by Federal organizations...is fused, validated, deconflicted, and approved for dissemination in a concise and, where appropriate, unclassified format." It was reported that DHS officials stated that the department has "...always sought ways to incorporate State and local officials by assigning them to offices within the Department, such as its intelligence office and its operations center." Homeland security officials reportedly stated that the presence of State and local officials at the ITACG would create "...unnecessary confusion at a unit whose main role is merely to package information."

²¹ According to New York City Mayor Michael Bloomberg, "The freedoms and opportunities that New York symbolizes mean that we remain a prime - if not the prime - target for al-Qaeda and other terrorist groups.... Yet, time and time again our appeals for fully risk-based funding have been ignored." Testimony before the Senate Homeland Security and Governmental Affairs Committee, Jan. 9, 2007.

should include the elimination of the disbursement of guaranteed funding minimums to all states and municipalities.²² Noting that HSGP grants “enhance States, territories, and Urban Areas ability to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies,”²³ others may argue that the continuation of a minimal level of funds to all states might be beneficial in shoring up vulnerabilities or buying equipment that can equally respond to man-made and natural threats to a jurisdiction, citizens, property, or government functions. Other commentators may maintain that disbursing a significant portion of the funds without regard to the risk level of a given locality will continue to impair the prevention, preparedness, and response capabilities of those cities deemed highest at risk.

Responsibility for Reducing Risk and Federal Grant Levels. Since its inception, DHS’s risk-based formula for distributing funds to state and local communities has been a source of frustration for members of the federal, state, and local governments²⁴ and those who assess post-9/11 counterterrorism program implementation efforts.²⁵ Some homeland security observers suggest that it is unrealistic to expect grant levels to continue to increase as U.S. budget concerns weigh on future appropriations. Others might note that as at-risk jurisdictions continue to shore up previously known vulnerabilities they will require less federal funding due to a lowering of their risk profile.

Table 1 below provides a cursory overview of the evolution of the DHS grant and risk assessment formula from FY2001 through FY2007.

²² Ibid.

²³ Homeland Security Grant Program, Department of Homeland Security. Available at [http://www.ojp.usdoj.gov/odp/newsreleases/HSGP_effectiveness_analysis.pdf], accessed Jan. 26, 2007.

²⁴ “Mayors, lawmakers press for more urban security funds,” *Government Executive*, June 21, 2006, available at [http://www.govexec.com/story_page.cfm?articleid=34377&ref=rrellink], accessed Jan. 26, 2007.

²⁵ National Commission on Terrorism Attacks Upon the United States (9/11 Commission), Recommendation 12.4 Protect Against and prepare for terrorist Attacks, p. 396. Available at [<http://www.9-11commission.gov/report/911Report.pdf>], accessed Jan. 26, 2007.

Table 1. Evolution of DHS Grant and Risk Assessment Formula

Agency - Period	Funding Proportion & Related Risk Assessment Formulas	
DOJ - Pre-9/11	Risk Allocation - Risk (R) = Population (P) (Defense Against Weapons of Mass Destruction Act of 1996, P.L. 104-201).	
DOJ - Post-9/11	Funding Proportion - (USA PATRIOT Act of 2001, P.L. 107-56) 40% Statutorily Mandated (.75% per state, Puerto Rico and Wash., D.C. + .25% per U.S. territory). The remaining 60% allocated by Risk - the assessment of which is statutorily unspecified. R=P. Funding formula, not to be confused with risk assessment formula used to determine the aforementioned 60% of the homeland security grants.	
DOJ/DHS - FY2002 & FY2003	40% Statutorily Mandated	60% allocated by Risk R = P
DHS - FY2004	40% Statutorily Mandated	60% allocated by Risk R = T+CI+PD ^a
Weighting of DHS - FY2004 Risk Formula	Threat (T) = Intelligence Community credible threats & FBI/ICE Field Investigations (weighted 3) Critical Infrastructure(CI) = (weighted 6) Population (P) = population/population density (weighted 9) ^b	
DHS - FY2005	40% Statutorily Mandated	60% allocated by Risk R = T+V ^c
Weighting of DHS - FY2005 Risk Formula	Threat (T) = Intelligence Community credible threats (2) & FBI/ICE Field Investigations (2) (weighted 4) Critical Infrastructure(CI) = (weighted 6) Population (P) = population/population density (weighted 9) *Additional factor = Mutual Aid Agreements (weighted 1)	
DHS - FY2006	40% Statutorily Mandated	60% allocated by Risk R = T*V*C. First year in which probability was systematically included in risk assessment.
Weighting of DHS - FY2006 Risk Formula	Risk is calculated for both geographic areas and assets. While both calculations include T, V, and C factors, they have distinct subcategories. <u>Geographic</u> <i>Threat (T)</i> - (IC reports, FBI investigations, ICE investigations, suspicious incidents, I-94 visitors from countries of interest, total # of visitors from such countries with state as destination) <i>Vulnerability (V)</i> - (total # international visitors, miles of international border, miles of designated WIPP route) <i>Consequence (C)</i> - (human health, economic, strategic mission, and psychological - as well as numerous subsets of each) <u>Asset</u> <i>Threat (T)</i> (strategic intent, 'chatter,' attractiveness of target, capabilities) <i>Vulnerability (V)</i> (value assigned by DHS) <i>Consequence (C)</i> (human health, economic, strategic mission, and psychological) It is not clear how each factor and sub-factor were weighted. ^d	
DHS - FY2007	40% Statutorily Mandated	60% allocated by Risk R = T*(V&C) ^e

Agency - Period	Funding Proportion & Related Risk Assessment Formulas
Weighting of DHS - FY2007 Risk Formula	<p><i>Threat (T)</i> = detainee reporting, on-going plot lines, Intelligence Community credible threats & FBI/ICE field investigations (weighted 20%)</p> <p><i>Vulnerability (V) & Consequence (C)</i> = (weighted 80% - the sum of the following factors:</p> <p><i>Population Index</i> - total population (nighttime, commuter, visitor, and military dependent) and population density - constrained to 50% impact (weighted 40%)</p> <p><i>Economic Index</i> (gross metropolitan product for UASI or %GDP for states (weighted 20%)</p> <p><i>National Infrastructure Index</i> (# Tier I Assets (X3) = # Tier II Assets) (weighted 15%)</p> <p><i>National Security Index</i> (presence of military bases + # of defense industrial base sites + international border crossings) (weighted 5%)^f</p>

Source: CRS presentation of DOJ and DHS Risk Assessment Formula.

- a. This was the first year DHS considered several sub-categories of data when calculating risk: current threat estimates (T), critical infrastructure (CI) assets within an urban area, and population density (PD)-related information.
- b. The P calculation appears to have initially focused on population, but later incorporated population density information.
- c. In FY2005, DHS added four more streams of data into the risk calculation. These seven categories of information have been represented in various forms and to various degrees in the subsequent formulas. See *DHS Risk Fiscal Year 2005 Homeland Security Grant Program: Program Guidelines and Application Kit*, p.1. What remains unclear is how the two variables (T and V) interact. Based on available information and discussions with DHS Officials, the relationship between T and V is assumed to be additive, as DHS did not move to a probabilistic risk formula until FY2006.
- d. It is clear that both the geographic and asset-based risk assessment scores were utilized to determine the total area/state risk score. U.S. Department of Homeland Security, "Overview of the FY2006 DHS Risk Analysis Methodology," 1-2. However, how those scores translated into grant allotments is uncertain.
- e. According to a DHS representative, due to the difficulties associated with differentiating levels of vulnerabilities across communities, DHS has effectively assigned a value of one to the vulnerability variable for each city and area. As a result, while DHS continues to use the FY2006 risk assessment formula of $R=T*V*C$, and state that risk is the product of three variables, in effect, the formula is $R=T*C$, and risk is the product of two variables.
- f. Risk continues to be calculated for both geographic areas and assets, but it is unclear how the aforementioned weighting changes affect each calculation, and how the two scores are used to determine grant allocation. U.S. DHS, "FY2007 DHS Grant Programs: Program Overview," p. 15.

To inform the ongoing congressional debate on risk assessment as it flows through the DHS grant program, the following section provides an assessment of some of the policy questions associated with risk assessment in a homeland security context.

Risk Assessment²⁶ and Resource Allocation — Macro Questions

The overview of the evolution of the risk assessment methodology as it pertains to homeland security grant allocations highlights a number of questions at the macro level, such as how to best measure risk, that might be considered before

²⁶ From a DHS perspective, risk assessment pertains solely to assessing the risk associated with terrorist attacks, not necessarily natural disasters.

contemplating questions of allocation. As mentioned above, the Commission recommended that the allocation of grants should be based on risk *and* (emphasis added) vulnerability. Vulnerability is but one of three elements of risk, as defined by DHS.²⁷ In recent Senate testimony, former Congressman and Vice Chair of the 9/11 Commission Lee Hamilton suggested that experience serve as a guide for risk assessment and resource allocation. Mr. Hamilton noted three elements worthy of consideration when allocating homeland security spending: (1) historical and empirical data on what has been attacked not only within the United States but overseas — Washington, DC; New York City, New York; Madrid, Spain; and London, England — all large cities; (2) Al Qaeda statements — according to Mr. Hamilton — “...So far as we know they (Al Qaeda) continue to target symbols of American power”; and (3) the best available intelligence.²⁸ While this approach is reasonable and based on sound logic, some might argue that broader questions and a more anticipatory approach may need to be considered to arrive at some credible and predictive value for future risk.

According to a recent RAND study, the following three questions might be addressed by policymakers before resource allocation decisions are made:

- Should resources be allocated based on risk, risk reduction, or some other basis?
- How can terrorism risk be estimated?
- What are the tolerable levels of risk?²⁹

Another fundamental question in this area is “what is the risk to” and “from what sources does the risk originate?” Is the risk to people, infrastructure, the economy, or all of the above? Is the source of risk acts of terrorism, or the broader “all-hazards” approach, where the interests lie in responding to “incidents of national significance,” as defined in the *National Response Plan*? Does DHS, as suggested by the department’s Inspector General, “need to continue refining its risk-based approach to award first responder grants that ensure the areas and assets that represent the greatest vulnerability to the public are as secure as possible?”³⁰

With respect to the threat element of the risk equation, to what extent is unique data collected by state and local officials being incorporated into the threat element of risk? State and local law enforcement and public safety personnel provide substantial amounts of data to DHS and other federal entities with the understanding that the information will be used, in part, to assess threat. Yet, according to a DHS official, the methodology for incorporating that data are under-developed and, as a

²⁷ It should be noted that quite often the terms risk, vulnerability, consequence, and threat are erroneously used interchangeably, as will be further discussed below.

²⁸ “Ensuring Full Implementation of the 9/11 Commission’s Recommendations,” a hearing of the Senate Homeland Security and Governmental Affairs Committee, Jan. 9, 2007.

²⁹ See Henry H. Willis, *Guiding Resource Allocations Based on Terrorism Risk* (A RAND Working Paper), March 2006.

³⁰ DHS Office of Inspector General, *Major Management Challenges Facing the Department of Homeland Security*, Dec. 2006, p. 8.

result, the data is not currently incorporated into threat assessment at the federal level in any systematic and meaningful manner.³¹ It may be possible that the emergence and proliferation of state, local, and regional intelligence fusion centers could become a funnel through which such state and local data could be aggregated and provided to the federal government in a manner that would allow it to contribute to threat assessment, an element of the risk equation that is weighted at 20% in FY2007.

The answers to these questions can have a fundamental impact on how grants are allocated. While the risk management process may be similar whether the source of risk is a hurricane or a terrorist attack, arguably, the inputs provided into the risk assessment model will be far different. DHS guidance shows that both the UASI and LETPP Programs are largely designed to provide state and local governments with funds to prepare and protect against as well as respond to and recover from acts of terrorism.³² While this purpose also exists in the SHSP, it has the additional purpose of supporting the implementation of the National Preparedness Goal. The other two grants currently under the Homeland Security Grant Program umbrella, the Metropolitan Medical Response System (MMRS) and the Citizen Corps Program (CCP), are almost completely focused on preparedness for post-event response. Consistent with a need to ensure all phases of a catastrophe are considered and program objectives are clearly defined, the DHS Inspector General found that “the department must incorporate sound risk management principles and methodologies to successfully prepare for, respond to, recover from, and mitigate acts of terrorism and natural disasters.”³³ In short, while DHS’s risk assessment methodology is largely geared toward countering terrorism, the results of the assessment, along with other factors, such as effectiveness, are used for purposes which go beyond terrorism.

Once the fundamental questions of “risk to” and “risk from what” are answered, it is necessary to form a methodology to measure relative risk and to draft and implement a strategy to reduce it. To this end and from an economic efficiency perspective, it could be argued that the optimal manner in which homeland security grants might be allocated would be according to a comparative analysis of how historical homeland security grants have actually reduced risk. From September 11, 2001, through FY2008, approximately \$12 billion will have been provided to state and local governments by DHS to prepare for and respond to terrorist attacks and other disasters.³⁴ A central question that may be asked is what has been the rate of return, as defined by identifiable and empirical risk reductions, on this \$12 billion investment? It does not appear, however, that there is an established methodology to engage in such analyses, nor are the data sets necessary for such analyses well-developed. According to one DHS official, while the department is planning to assess the impact of DHS grants on risk reduction in FY2008, it has been somewhat constrained by resources and the absence of a methodology to conduct such an

³¹ Interview with DHS Official, Jan. 9, 2007.

³² DHS *FY2007: Homeland Security Grant Program: Program Guidance and Application Kit*, Jan. 2007, pp. 1-2 and A1-A4.

³³ *Ibid.*, p. 8.

³⁴ DHS, “DHS Announces \$1.7 Billion in Homeland Security Grants,” press release, May 31, 2006.

assessment.³⁵ As a result, some might argue, the next best method to allocating resources is to assess, measure and rank relative risk. This is, in essence, the approach currently being used by DHS.

Risk Management and Assessment: Complex Activities

The concept of risk - how to define, assess, and manage it - is relatively complex. According to DHS, "...Risk is classically represented as the product of a probability of a particular outcome and the results of that outcome."³⁶ As mentioned above, it was not until FY2006 that DHS moved from a risk-like or additive approach to assessing risk to one that is guided by more classically defined or probabilistic methods of assessing risk. As will be expanded upon below, DHS differentiates between two different, but complementary types of risk: asset-based risk and geographic-based risk. Because DHS is assessing risk as a means to allocate resources to buy down risk, it is imperative, according to DHS, that its risk calculations be relative. That is, "...Because of the dynamic nature of temporal valuations in the many elements that figure into risk, an absolute value, even if it could be calculated, would be meaningful for a very limited time."³⁷ Moreover, DHS differentiates between risk analysis and risk management. According to the Society for Risk Analysis:

Risk analysis is broadly defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and

³⁵ Interview with DHS Official, Jan. 9, 2007.

³⁶ DHS, Directorate of Preparedness, Risk Management Division, and DHS Office of Grants and Training, *Risk Analysis for Fiscal Year 2006 Homeland Security Grants*, p. 4.

³⁷ Ibid., p. 2. For the relatively parochial purpose of allocating homeland security grant resources, absolute risk may be of marginal utility. However, the absolute risk to a certain critical asset or infrastructure may be highly relevant to state, local and private sector officials. For example, risk management analyses have been conducted on the terrorist threat to liquefied natural gas (LNG) terminals in the United States. See Richard A. Clarke, *LNG Facilities in Urban Areas: A Security Risk Management Analysis for Attorney General Patrick Lynch Rhode Island*, May 2005. See also Carl Southwell, Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, *An Analysis of the Risks of a Terrorist Attack on LNG Receiving Facilities in the United States*, Nov. 9, 2005. Because the risk analysis is conducted for one set of assets, Clarke, et.al. use numerous variables including intent, capabilities, vulnerabilities, consequences and recovery to assess security risk. These variables are, of course, relevant to assessing relative risk as well. However, in order to assess the attractiveness of LNG terminals as a target, Clarke uses the U.S. military - Special Operations Force's CARVER target selection model. CARVER stands for criticality, accessibility, recuperability, vulnerability, effect and recognizability (See Field Manual 34-36 *Special Operation Forces Intelligence and Electronics Warfare Operation*, Sept. 30, 1991). The aforementioned Rhode Island LNG report states (p.76) that "...Since we are aware that al Qaeda has adopted much of U.S. Army doctrine for use in its training camps, it is fair to assume the principals in the CARVER matrix apply to their targeting." With its highly tactical focus on specific assets and characteristics of those assets, this model may have limited utility for the relative homeland security risk assessments.

to society at a local, regional, national, or global level. Risk analysis seeks to inform, not to dictate, the complex and difficult choices among possible measures to mitigate risks.³⁸

Risk *management* is a continual process or cycle in which risks are identified, measured and evaluated; countermeasures are then designed, implemented and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and avoidance.³⁹ Risk *assessment* pertains to the quantification or measurement of identified risk and probabilistic assessment that certain risks will manifest themselves.⁴⁰ According to the Government Accountability Office (GAO), risk assessment is:

the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. It is a function of threat, vulnerability and consequence. A risk assessment may include scenarios in which two or more risks interact to create greater or lesser impact. A risk assessment provides the basis for the rank ordering of risks and for establishing priorities for countermeasures.⁴¹

The practice of risk management is well-developed within the insurance, engineering, finance, and political risk industries. It is clear, however, that risk management remains relatively immature in its application to the homeland security field. Some might argue that the implementation of risk assessment and management in the homeland security and counterterrorism fields may be more complex than in its industrial application where the primary objective is to protect against financial loss. Financial loss is, of course, one element of assessing and mitigating risk in a homeland security context, but of equal if not more importance are threats to human health and strategic national missions, among other factors. According to DHS, the following issues must be taken into consideration in the assessment of risk in the homeland security context:

- *Historical Data.* In the insurance or financial sectors, the assessment of risk benefits from a rich and voluminous set of data which can be mined for patterns of historical behavior. While there are various governmental and non-governmental databases on terrorism, these data sources are relatively less robust. As a result,

³⁸ Society for Risk Analysis. Available at [<http://www.SRA.org>], accessed Jan. 26, 2007.

³⁹ This definition is derived from (1) Yacov's definition of risk management (see Yacov V. Haimes *Risk Modeling, Assessment, and Management* (2nd) (John Wiley & Sons, 2004), p.57-58) and (2) *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, (GAO 06-91), Dec. 2005, p. 111.

⁴⁰ See Yacov V. Haimes *Risk Modeling, Assessment, and Management* (2nd) (John Wiley & Sons, 2004), p.57-58.

⁴¹ See *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, (GAO 06-91), Dec. 2005, p. 111.

the subjective judgment of intelligence and terrorism experts become relatively more important in the projection of likely threat scenarios directed against categories of assets and/or geographic areas.

- *Risk “Inheritance.”* Because grant candidates include states and Urban Areas, and individual assets exist in both spaces, risk can be “inherited” from one candidate to another. For example, the risk score for a port will be “inherited” by the city and state in which that port is located. As such, according to DHS, it utilizes various mathematical techniques, including weighting, normalization and order of computation to control for such unique factors.⁴²

There are numerous other complicating factors associated with assessing risk in the homeland security context.⁴³ Notwithstanding a common framework for assessing risk at an aggregate level, one of the central problems is that risks need to be defined at a micro level — for example, the risk to a certain asset or geographic area, given terrorist capabilities and intentions — to be very useful.⁴⁴ At least with respect to assessing risk from terrorism, the nature of the risk is dynamic, as terrorists continually monitor successful countermeasures and adapt their targets, tactics, and modes of operation to surmount the countermeasures. Moreover, as alluded to above, a related problem is the absence of a definitive answer to the question of “how much risk is acceptable?” Secretary Chertoff has been open and frank in discussing the department’s risk-based approach - that is - the fact that the country has to accept some level of risk, as it is not feasible to protect against every real or perceived risk. Yet that level of acceptable risk, the threshold over which federal resources will be dedicated to managing risk, is not yet defined.⁴⁵ In short, the successful risk reduction measures of today, may not necessarily be as successful in the near-to-medium term.

⁴² DHS, *Risk Analysis for Fiscal Year 2006 Homeland Security Grants*, pp. 8-12.

⁴³ See Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, Jamison Jo Medby, *Estimating Terrorism Risk*, RAND Center for Terrorism Risk Management Policy (2005). See also *Managing Terrorism Risk in 2004*, Risk Management Solutions, Inc., Newark, CA.

⁴⁴ If risk is equal to threat*vulnerability*consequence, by mathematical principle if any value on the right side of the equation is assessed to be zero, risk is also zero. For example, because the vulnerability of a bridge to a chemical attack is zero, the risk to bridges from chemical attacks is also zero.

⁴⁵ Some would argue that given the statutory formula in the USA PATRIOT Act (P.L. 107-56, §1014, codified at 42 U.S.C., §3711) stipulating that .75 percent of the total amount of grants shall be allocated to each state (plus the District of Columbia and Puerto Rico), and .25 % for the territories of Guam, American Samoa, Northern Mariana Islands, and the Virgin Islands, the risk threshold is minimal, as this formula assumes that all states experience some level of risk and receive funding as a result. As will be discussed in the options section of this report, whether this funding was intended to be perpetual, or to bring all states up to a minimal level of security and capability, and then allow the states to assume financial responsibility for continued operations and maintenance of established security programs and activities, may be an issue for the 110th Congress. In FY2006, this .75% formula equates to 40% of the total \$1.7 billion homeland security grant appropriation.

As will be outlined below, even if there is agreement on the central elements of risk, these elements are not necessarily independent of one another, thus requiring a sophisticated understanding of how each of the elements or variables of risk are interdependent.⁴⁶ Stochastic and sensitivity tests for each variable and regression between variables may be of some utility in understanding how strong the relationships between variables are.⁴⁷ For FY2007, as mentioned above, DHS has in effect assigned a value of one to vulnerability. While understandable at some level, this essentially eviscerates any interplay between vulnerability and consequence by having the effect of weighting the consequences of such an attack at 80%. It could be argued that if the vulnerability of a particular asset is exceedingly low, regardless of how grave the consequence, the risk to the asset may also be very low and, therefore, allocating relatively scarce homeland security resources to such an asset may be inefficient and ineffective.

Insofar as measuring risk is concerned, it could be argued that it is essential to identify the primary drivers of risk and collect the most appropriate data to quantify those risks. Collecting and measuring data that is readily available, but not central to risk yields quantifiable risk scores, yet some could argue that the results would be indefensible and relatively meaningless. If data which drive risk are not currently being collected, perhaps in the short-term such data deficiencies might be clearly recognized and controlled for in calculating risk. Reducing a variable value to zero or one based on the difficulty of collecting appropriate data to measure that variable should only be used as a temporary, stop-gap technique, as invariably such practices result in inaccurate risk assessments. Moreover, the level of confidence decision-makers have in data collected to assess risk is important. Resource allocation could be based, for example, *solely* on population figures, a statistic for which high confidence data exists. However, detriments of such a system are that population, *in and of itself*, may not necessarily be a terrorist target. If the population is not particularly dense, or exists in an area of marginal national economic impact or exists in an area where there are few critical national infrastructure assets, the population may not necessarily be a target for various terrorist groups.

There may be a balance to be struck between a risk assessment methodology that is too simple and one that is too complex. The question is what is the appropriate balance, and how a consistent methodology can be applied to a dynamic set of

⁴⁶ Yacov Y. Haimes, founding director of the Center for Risk Management of Engineering Systems at the University of Virginia argues “Quantitative risk assessment and management cannot be conducted on an ad hoc basis or by addressing selective sources of risk.” This engineering or systems based approach may be one of the areas where there is a commonality between an engineering approach to risk management and a homeland security approach, as terrorist threats, infrastructure vulnerabilities and the consequences associated with a successful attack are also inter-related. See Yacov V. Haimes *Risk Modeling, Assessment, and Management* (2nd) (John Wiley & Sons, 2004), p.18.

⁴⁷ Bayesian probability represents the degree of belief that an event will occur, and has been used by some in assessing the probabilities of a successful terrorist attack against a target. In Bayesian analysis, investigators assess the current state of knowledge regarding the issue of interest, gather new data to address remaining questions, and then update and refine their understanding to incorporate both new and old data. See [<http://www.bayesian.org/>], accessed Jan. 26, 2007.

terrorist threats. Some homeland security observers might argue that the development of a long-term risk assessment strategy implemented by a strong DHS or broader government risk assessment analytic center that has as its sole mission the study of risk — its inputs and assessment of risk reduction results — may prove highly useful to help achieve this balance.⁴⁸ Regardless of the complexity of the risk assessment methodology, due to the inherent uncertainties associated with assessing risk in a dynamic counterterrorism context, some level of flexibility in managing risk may be necessary. Empirical data based on historical terrorist attacks in the United States may, therefore, continue to play an important role in resource allocation designed to buy down risk. Some might argue that such an approach constitutes a “rearview mirror” or reactive perspective. Others might argue that unless and until reliable intelligence can demonstrate otherwise, historical attack patterns, informed by the best available current and strategic intelligence, will remain an essential risk assessment indicator.

Risk Assessment: Some Critical Drivers and Perspectives

Numerous factors drive risk and are essential to understanding risk assessment and management. This section will provide some basic definitions common to the risk assessment and management field. Although they are often used interchangeably, the terms associated with risk assessment have unique, though related, meanings. The most recent data available is included in the *FY2007 Homeland Security Grant Program - Grant Guidelines and Application Kit*, in which it is stated that:

Risk will be evaluated at the Federal level using a risk analysis model developed by DHS in conjunction with other Federal entities. Risk is defined as the *product* of three principal variables: (1) Threat, or the likelihood of a type of attack occurring, (2) Vulnerability, or the relative exposure of an attack and (3) Consequence, or expected impact of an attack.⁴⁹

As alluded to above, DHS also differentiates between the following two types of risk, the attributes of which are depicted in **Figures 3 and 4** below:

- *Asset-Based Risk* “...employs strategic threat estimates from the Intelligence Community of an adversary’s intent and capability to attack different types (e.g. chemical plants, stadiums, commercial airports) using different methods of attack. The vulnerability of each

⁴⁸ In a related organizational development, the Homeland Security Advisory Council recently recommended that DHS establish an Office of Net Assessments to “...provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats.” Ostensibly, this office would also work with the Director of National Intelligence to develop a comprehensive National Intelligence Estimate to address threats to the homeland. See *Homeland Security Advisory Council, Future of Terrorism Task Force*, Jan 11, 2007, p.7. Any such office would apparently work closely with a potential risk assessment center, particularly with respect to assessment of terrorist threats and the means to combat such threats using, among other tools, the homeland security grants.

⁴⁹ *FY2007 Homeland Security Grant Program - Grant Guidelines and Application Kit*, p.8.

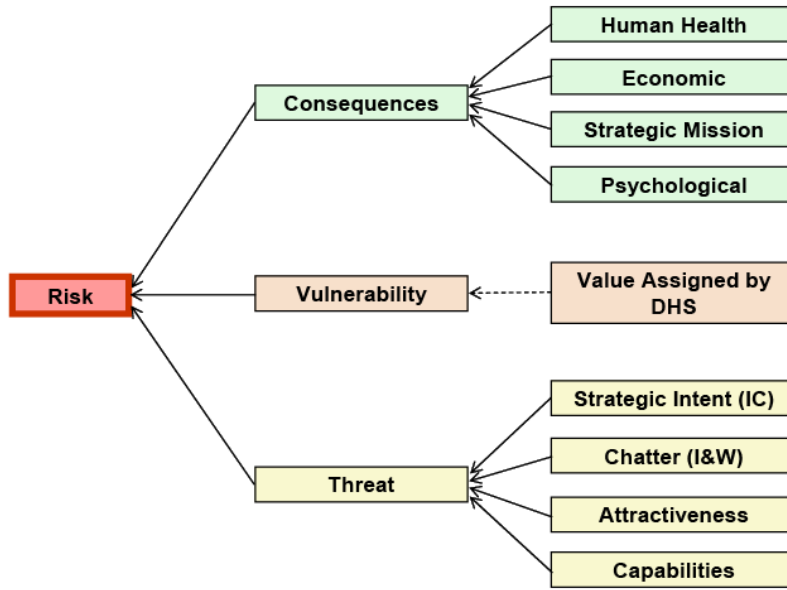
asset type to each attack method is analyzed to yield the form of attack most likely to be successful.”⁵⁰

- *Geographically-Based Risk* “..considers general characteristics associated with a geographic area independent of the assets that exist within that area. This type of risk evaluates reported threats (credible and less credible), law enforcement activity (FBI and ICE terrorism case data and suspicious incidents)... Vulnerability factors considered include international border, number of international visitors and port channel length. The consequences of an attack on that area are then estimated to include human health...economic...strategic mission... and psychological impacts.”⁵¹

⁵⁰ DHS, *Overview of the FY2006 DHS Risk Analysis Methodology*, p.1.

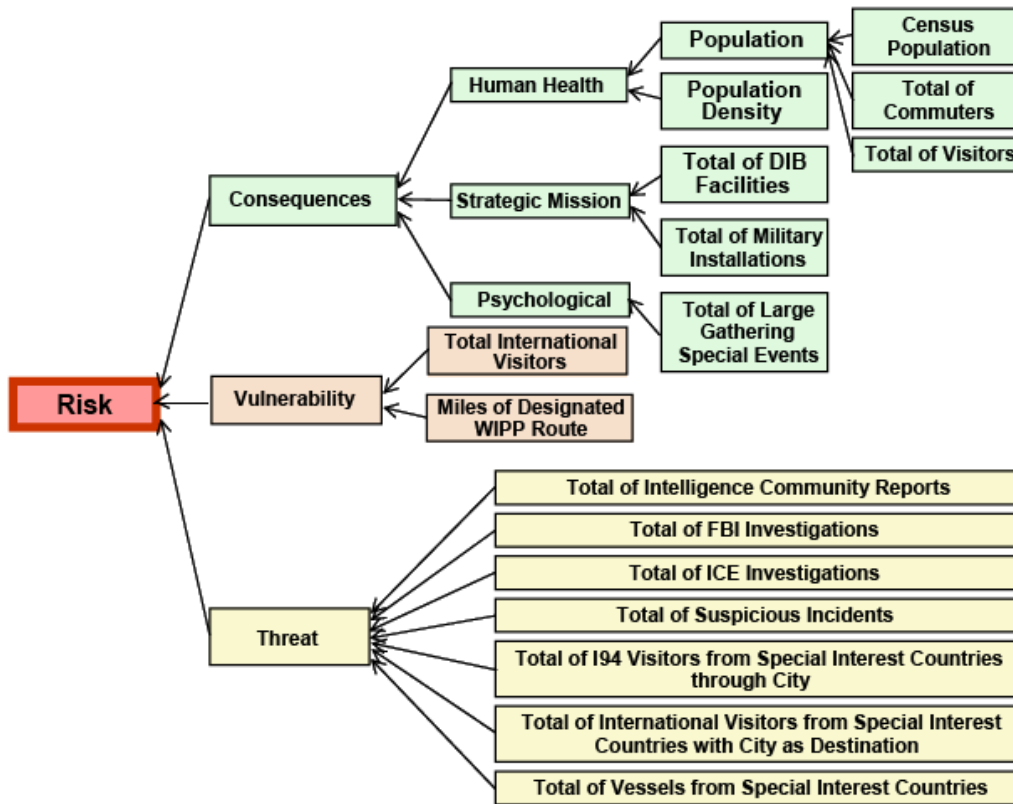
⁵¹ Ibid.

Figure 3. Asset-Based Risk Analysis Attributes



Source: CRS presentation of DHS risk analysis attributes.

Figure 4. State Geographic Risk Analysis Attributes



Source: CRS presentation of DHS risk analysis attributes.

In short, as alluded to above, the DHS formula for assessing risk, whether it is asset-based or geographic-based, is: *Risk = Threat*Vulnerability*Consequence*, otherwise expressed as,

$$R=T*V*C$$

This formula is central not only to the allocation of DHS grant programs, but to all of the department's activities, as Secretary Chertoff has stated.⁵² It is important to define these variables for a number of reasons:

- Without a common understanding of the lexicon, it is difficult to assess risk at the strategic and tactical levels.
- In order to gather the appropriate data which serves as an input to the risk assessment process, state and local agencies must understand how DHS is defining the elements of risk.
- In the absence of an understanding of each of these elements individually, it becomes increasingly difficult to comprehend how they are inter-related and inter-dependent.

There are numerous DHS elements, including the U.S. Coast Guard, Office for Domestic Preparedness and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), among others, that are responsible for risk analysis and management.⁵³ An example of how one component defines and practices risk assessment is instructive. HITRAC is the entity within DHS that is tasked with combining intelligence threat data as assessed and accessed by the DHS Office of Intelligence and Analysis with infrastructure vulnerabilities. According to a HITRAC Representative:

While inherently the most subjective component of the risk equation, threat of enemy attack is derived from study of enemy intent and capability. Intent of this adversary is assessed after study of all available information about they want to accomplish by attacking the United States. We work with our partners in the intelligence community to understand as much as we are able about the terrorists' goals, plans, and desires. We match what we know about the intentions of the adversary with information we have about what the enemy is capable of accomplishing. For this part of the equation we rely both on what we

⁵² On Nov. 28, 2006, Secretary Chertoff stated "I'm going to repeat something I've said a lot in the almost two years I've been on this job, which is the core principle that animates what we do at DHS and this is risk management. It is a recognition of the fact that management of risk is not elimination of risk. There is no elimination of risk in life...." Keynote Address by Secretary of Homeland Security Michael Chertoff to the 2006 Grants & Training National Conference.

⁵³ See General Accountability Office, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructures*, GAO-06-91, Dec. 2005. GAO reviewed the risk practices of these three DHS elements and concluded, in part, that "progress in risk management is affected by organizational maturity and the complexity of the risk management task."

see the enemy discussing, recruiting and training for as well as lessons learned from overseas attacks....⁵⁴

This is just one example of how a single entity within DHS is approaching risk and specifically defining its components. It should be noted that although DHS headquarters has adopted a particular risk methodology, it is unclear how pervasive that approach has become outside headquarters, specifically within agencies brought under the department in 2004.

Given the evolution of DHS's risk assessment methodology and associated complexities translating risk assessments into well-targeted allocations of HSGP funds to buy down risk, there are a number of possible approaches for Congress to consider in this area.

Possible Approaches for Congress

More than natural disasters, assessing risk emanating from manmade actions is an extremely difficult task. Methodological tension is created when attempting to apply a quantitative formula to human-driven activities that require subjective assessments of enemy capabilities and intentions. Were a truly effective risk assessment tool to be created to help decision-makers manage risk, it would have to recognize that "management of risk is not elimination of risk."⁵⁵ Whether focused on an "all-hazards" or counterterrorism approach, tools that attempt to quantify risk will always be inexact. However, sound data, a well thought-out formula, and consistent application of the methodology are important when attempting to measure terrorism risk to the U.S. and systematically buy down the risk to a particular location or asset. Such clarity and consistency are particularly important as the funds granted based on the DHS's risk methodology are the primary tools the federal government has to influence the behavior of state and local partners who will be the first on the scene of a terrorist attack and will be responsible for returning the community to pre-incident conditions. Congress has a number of apparent options concerning DHS's risk methodology efforts, including the following:

⁵⁴ See testimony of Melissa Smislova, Acting Director HITRAC, before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Nov. 17, 2005. How subjective data are treated; the extent of expert input into a strategic, dynamic, and continual risk assessment process; the continually updated weighting of various factors; and the presence of *both* intent and opportunity are all critical elements of the risk assessment process. Whether HITRAC has the appropriate mix of personnel, resources, and singularity of focus on risk assessment methods to serve as a potential, permanent DHS entity to continually refine and implement a dynamic risk assessment model is an open question.

⁵⁵ Michael Chertoff, DHS Secretary, Keynote Address by Secretary of Homeland Security Michael Chertoff to the 2006 Grants & Training National Conference, Nov. 28, 2006. Available at [http://www.dhs.gov/xnews/speeches/sp_1164738645429.shtm], accessed Jan. 26, 2007.

Maintaining Status Quo. Congress may wish to maintain the current policy and practices associated with DHS's existing risk assessment methodologies, and their affect on HSGP allocations. Some might argue that in the absence of measures to assess historical effectiveness of DHS grant programs, changing formulas and methodologies may be premature. Others might argue that with more than \$12 billion worth of investment aimed at risk reduction and preparedness, state and local governments should have achieved a level of preparedness and capability that can allow room for negotiation on financial burden-sharing with the federal government for those programs deemed worthy of future support.

National Impact Assessment. By FY2008, more than \$12 billion will have been provided to states, localities, and regions to buy down risk and enhance preparedness and capabilities to prevent a terrorist attack or to respond to such an attack or natural disaster should one occur. While audits have been conducted to determine how allocated funds have been spent, a national assessment of how much risk has been reduced as a result of such expenditures has not been undertaken. How much has risk been bought down? What investments have yielded the highest rate of return? What is the risk profile of each grant recipient moving forward? How are their existing capabilities measured against extant risk? What capabilities gaps exist, and how can resources best be targeted to address those gaps? There are at least two possible precursors to the drafting of such an impact assessment: (1) a defensible methodology that can (a) reasonably define and measure risk, (b) provide a means for measuring how developing capabilities are reducing that risk, and (c) illustrate how to identify specific capability gaps which might serve as an input for future allocation of homeland security grants; and (2) articulation of this methodology, including the data necessary to conduct such an assessment, to grant recipients. With the results of such an assessment, federal, state, local, and regional authorities might arguably be in a better position to understand the most effective and efficient way to target relatively scarce homeland security resources.

Further Enhance Transparency. While safeguarding the intelligence, law enforcement, and other sensitive information weighted and analyzed through DHS's risk methodology, disclosure of the mathematical equation used to determine threat, vulnerability, and consequence may allow all applicants and stakeholders to understand and have a basis to confirm or challenge the results prior to funds being allocated. It could be argued that providing this level of detail regarding the methodology and underlying equation may allow those who would seek to attack U.S. facilities to reverse-engineer the formula, thus increasing the probability of a successful terrorist attack. Others might maintain that allowing the risk formula equations to be revealed would encourage state and municipalities to manipulate the data provided to DHS, thus increasing their chances of receiving additional funding without a sufficient risk-based justification. Homeland security observers could counter these arguments by suggesting that though there may be the potential for those wishing to take advantage of the transparency of the system, the positives include possible increases in information sharing between DHS and state and local governments due to an understanding of how data is used and as such result in increased confidence in the other entity. Some could argue more transparency would allow DHS to more confidently allocate resources, as enhanced transparency may reduce the surprised outcries that seem to arise with each cycle's award announcements. This argument is based on the assumption that grant applicants that

are comfortable with the risk assessment process and familiar with the data streams used to calculate risk. As a result, the applicants may be less likely to be surprised by their jurisdiction's ranking and awards.

Development of a Risk Strategy Both Within DHS and Throughout All Government Agencies. Since the establishment of DHS in March of 2003, the department's risk formula has evolved. Though it could be argued that these changes are indicative of a maturing organization and process, it is possible that the lack of a coherent, long-term, overarching risk strategy, which forms the foundation of departmental activities, could have negative repercussions for buying down risk. Without a clearly articulated risk methodology based on fundamentals intrinsic to risk, yet adaptive to changing threats, a baseline understanding of the nation's risk profile may never be achieved and the department's risk assessment process could potentially be vulnerable to budget fluctuations and political influence. This is especially important given the apparent division of risk assessment responsibilities throughout various offices and directorates within the department.

Arguments can be made that such an overarching risk philosophy needs to be adopted throughout the federal government. In a December 2005 report on homeland security risk management, GAO concluded that

for the results of a risk management system to be meaningful and useful, all related agencies should be using similar methods. If agencies' methods are not compatible, then comparisons between agencies become difficult and sector or national risk assessments becomes less reliable. In our earlier work, we concluded that a structured, systematic approach to risk management offers the best assurance that activities designed to protect the homeland and combat the effects of terrorism will produce the most effective and efficient results.⁵⁶

A cohesive risk strategy and agreement on core terms amongst disparate agencies is desirable because many aspects of the risk assessment process are dependent on functions performed by agencies outside the department.⁵⁷ However, the necessity of common definitions and standards goes beyond the federal government. As states and localities continue to provide information to be included in the risk assessment

⁵⁶ U.S. Government Accountability Office (GAO), Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,"GAO-06-91, Dec. 2005, available at [<http://www.gao.gov/new.items/d0691.pdf>], accessed Jan. 26, 2007.

⁵⁷ A hypothetical example is provided by examining the FY2007 risk formula weights. This year's formula assigns a 20% weight to the Threat (T) variable. Threat is determined using a variety of data points, to include detainee reporting, on-going plot lines, credible threat reporting, and investigations. The investigations portion of the threat variable is comprised of terrorism investigations-related information provided by the FBI and Immigration and Customs Enforcement (ICE). Hypothetically, if the FBI and ICE did not operate using the same conception of what constitutes a terrorist threat and/or utilized alternate metrics to determine source credibility and determine corroboration, the output of DHS's risk assessment could be skewed. This is just one of many potential unintended negative consequences that can occur if federal agencies involved in aspects of the risk management process are not operating using the same definitions.

process, to include, information on critical infrastructure sites within their respective jurisdictions and, eventually, investigative information, the rationale for attempting to develop national-wide risk assessment strategy at all levels of government becomes stronger.

Appointment of a DHS Risk Assessment Manager (RAM). With regards to DHS's risk assessment efforts, the department might potentially create a Risk Assessment Manager (RAM) position charged with better integrating the various elements working on aspects of the risk assessment process. In addition, the RAM might be assigned the responsibility of creating and subsequently implementing a department-wide strategic risk strategy. Such a position could be in an advisory capacity to the Secretary or entail operational and oversight functions of a permanent DHS Risk Assessment Center (see below). The creation of a RAM within DHS responsible for coordinating all inter-departmental risk methodology activities would provide Congress, other federal government agencies, and state and local homeland security leaders with a single person accountable for explaining the complexities of future risk management strategy efforts and a specific office to receive suggestions regarding improving current processes. The RAM could also serve in a liaison capacity to ensure external agencies are familiar with DHS's approach to risk and facilitate agreement on key terms and processes amongst other agencies.

Creation of a DHS Risk Advisory Board (RAB). As previously stated, Secretary Chertoff has made it clear that risk assessment underlies all elements of the department's operations. Risk management and assessment are disciplines which are relatively well-developed across the private sector. Moreover, within the U.S. government, there are numerous experts on risk assessment. To ensure that the Secretary is getting the best possible advice as to how DHS should continue to refine its risk management activities, a formal board of senior-level risk management professionals might be established to advise the Secretary. While not having program management responsibilities, the Risk Advisory Board (RAB) might advise the Secretary on the best risk management practices across industry and government. It could also lead the DHS effort, with substantial input from a potential Risk Assessment Center (see below), to draft a long-term risk management strategy.

Creation of a Permanent Risk Assessment Center (RAC). While the proposed RAB would operate on a strategic level, it could be beneficial for DHS to examine its current efforts to apply risk strategy to its various programs and initiatives. Risk is central to DHS's operations. DHS may not necessarily have the appropriate resources dedicated full-time to (1) pro-actively assess the dynamic drivers of risk, (2) lead the collection of the right types of data to assess risk, and (3) develop a methodology to analyze how effectively past homeland security grant investments have "bought down" risk. These tasks are relatively complex and, it could be argued, require the formation of a group of professional methodologists whose sole function is risk assessment. While elements of this capability may exist now within the Preparedness Directorate, no single group has this sole responsibility. For example, HITRAC is charged largely with mapping vulnerabilities to threats, which is an essential function unto itself.

There are several potential benefits offered by a risk center: First, a permanent center would likely help DHS to think strategically about the current risk assessment process. Second, continued attention to this issue and sufficient time to address it would probably allow DHS to create more effective assessment tools and use those multiple tools in tandem to analyze various risk areas. Third, the risk center would potentially allow DHS to draw on the existing expertise and resources of all the offices and divisions within DHS, as well as external entities, such as other Intelligence Community agencies.

Implement 9/11 Commission Recommendation. As mentioned above, the 9/11 Commission recommended that “...homeland security assistance should be based strictly on an assessment of risks and vulnerabilities...But federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support.”⁵⁸ Some homeland security observers could interpret this literally to mean that after six years and \$12 billion of homeland security investments, most states should be at some minimal level of security and capability. Therefore, some might argue, the time may be appropriate to revisit the USA PATRIOT Act formula which results in 40% of the total DHS grant funding being allocated based on formula which is not based primarily on risk. Others might argue that until a methodology is developed to ascertain how prior years’ grant allocations have decreased each state’s risk levels, it may be premature to alter the formula. Questions that might be addressed when considering this options include

- What duration did Congress originally intend when it created the DOJ and now DHS homeland security grants?
- What measures are in place to ensure that state and local governments are spending resources in a manner that is consistent with congressional intent?
- To what extent, if at all, has congressional oversight yielded any indications that state and local governments have come to view homeland security grants as entitlements?
- Has DHS or Congress entered into discussions with state and local governments about sustainable burden-sharing arrangements with respect to state and local programs assessed as being worthy of continued financial support?

Treat Terrorism Prevention Grants Uniquely. Secretary Chertoff recently stated that one of the unique areas in which the DHS can add value is in the area of prevention. He stated, “...obviously, when it comes to terrorism, our best solution is a solution that prevents a terrorist act before it actually comes about. And a critical element in that is our early warning system, which is intelligence....”⁵⁹ Notwithstanding this statement, a review of aggregate budget data for homeland

⁵⁸ National Commission of Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission of Terrorist Attacks Upon the United States*, Authorized Edition (New York: WW Norton and Company, 2004), p. 396.

⁵⁹ Keynote Address by Secretary of Homeland Security Michael Chertoff to the 2006 Grants & Training National Conference, Nov. 28, 2006.

security expenditures suggests that less than 1% of what the U.S. government spends on homeland security is dedicated to intelligence and warning, an essential element in the prevention component of homeland security.⁶⁰ While there are many similarities in the response capability, whether the response be to a successful terrorist attack or natural disaster, terrorist acts can be prevented, natural disasters cannot. Information related to meteorology is different from intelligence related to national security. The threat element of the risk reduction formula is what differentiates terrorism from all other hazards. As mentioned throughout this report, terrorist threats are dynamic and evolve over time; some might argue the risk assessment methodology and attendant grant allocation process should be as agile as the adversary against which its resources are directed. DHS currently has an *Intelligence Enterprise Strategic Plan*, and the FY2007 grant application kit provides guidance for state, local and regional intelligence fusion centers. Yet, the linkages between these two documents and the grant process, some would argue, is tenuous. One of the Homeland Security Presidential Directive (HSPD)-8 derived “Universal Tasks” is prevention. Drawing upon the *National Strategy for Combating Terrorism*, Congress may ultimately consider recommending that DHS provide a specific and articulable strategy and approach to terrorism prevention, which would include a focus on how the grant allocation process is tailored to fully leverage intelligence across levels of government to *prevent* terrorist acts.

⁶⁰ See Office of Management and Budget, *Analytical Perspectives: Budget of the United States Government Fiscal Year 2007*, Table 3-2, p. 33. Intelligence and warning is one of six critical mission areas outlined in the *National Strategy for Homeland Security*. There is at least one caveat to these figures. While the figures for the intelligence and warning include those reported by the Departments of Defense and Justice and the Intelligence Community Management Account, other Intelligence Community funds dedicated to the homeland security intelligence and warning function might not be captured in the OMB data.

Appendix. Legislative Activity on DHS Risk Formula for Grants

	S. 1013 Homeland Security FORWARD Funding Act of 2005 109th Congress	S. 21 Homeland Security Grant Enhancement Act of 2005 109th Congress	H.R. 1544 Faster and Smarter Funding for First Responders Act of 2005 109th Congress	H.R. 1 Implementing the 9/11 Commission Recommendations Act of 2007 110th Congress	S. 4 Improving America’s Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007 110th Congress
Statutory Minimum Allocations	<p>50 States, DC, & Puerto Rico (PR)^a = 0.25% of the SHSGP monies, while the four US territories receive 0.08% of the SHSGP funding. No other grants are mentioned in this section.</p> <p>TOTAL GUARANTEED = 13.32% of SHSGP allotment</p> <p>*Includes: SHSGP, UASI, LETTP, and CCP.</p>	<p>50 States & DC = the greater of either (1) 0.55% of all appropriated funds, or (2) the state’s sliding scale baseline allocation^b multiplied by 28.62% of the total amount appropriated for the Threat-Based Homeland Security Grant Program. PR = 0.35%, and the four US territories = 0.055%.</p> <p>TOTAL GUARANTEED= 28.62% based on option (1), option 2 was not calculated</p> <p>*Includes: SHSGP, UASI, and LETTP.</p>	<p>Most States^c & DC and PR will receive 0.25% for covered grants, however states that qualify as having “additional high-risk qualifying criteria” will receive 0.45%. Four US territories will receive 0.08% and directly eligible tribes would receive 0.08%.</p> <p>TOTAL GUARANTEED= between 13.32% - 23.72% plus whatever percentage is awarded to directly eligible tribes.</p> <p>*Includes: SHSGP, UASI, LETTP, and CCP</p>	<p>50 States, DC, & PR^d are insured to receive no less than 0.25% and those that have an approved plan and meet at least one of the “additional high risk criteria”^e will receive no less than 0.45% of the funds available for covered grants for that fiscal year. The four US territories will receive no less than 0.08%.</p> <p>TOTAL GUARANTEED= between 13.32% - 23.72%</p> <p>*Includes: SHSGP, UASI, and</p>	<p>SHORT TITLE. This act may be cited as the ‘Improving America’s Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007’. SEC. 2. SENSE OF CONGRESS. It is the sense of Congress that Congress should enact, and the President should sign, legislation to make the United States more secure by implementing unfinished recommendations of the 9/11 Commission to fight the war on terror more effectively and to improve homeland security.</p>

	S. 1013 Homeland Security FORWARD Funding Act of 2005 109th Congress	S. 21 Homeland Security Grant Enhancement Act of 2005 109th Congress	H.R. 1544 Faster and Smarter Funding for First Responders Act of 2005 109th Congress	H.R. 1 Implementing the 9/11 Commission Recommendations Act of 2007 110th Congress	S. 4 Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007 110th Congress
Risk Funding	The bill creates a Homeland Security Grants Board to allocate the remaining funds based on an annual prioritized "risk-based ranking," which is based on the degree to which the monies would enhance essential capabilities to lessen the threat, vulnerability, and consequences of attack. ^f	The bill does not stipulate how the remaining funding would be allocated.	The bill contains almost the exact language as S. 1013 with regards to a similar Board to allocate the remaining funds based on a "risk-based ranking" and prioritizing terrorist threats.	The bill directs the Secretary of Homeland Security to "evaluate and annually prioritize all pending applications for covered grants...based upon the most current risk assessment available..."	

Source: CRS presentation of select legislation in the 109th and 110th Congress.

- a. There is a requirement for states to have a security plan in order to qualify for the automatic grant allocation minimum- "Each State that has an approved State homeland security plan receives no less than 0.25 percent of the funds available of the State Homeland Security Grant Program."
- b. The sliding scale defined in Section 1801, "represents each states's weighted share (where weighting is done based on a combination of population and population density) of the pot of money (28.62%) that results from adding together the 0.55% minimum distribution to each state, plus the amounts allocated for the District of Columbia and the remaining territories." Homeland Security Grant Enhancement Act of 2005, report of the US Senate Committee on Homeland Security and Governmental Affairs to accompany S. 21, S.Rept. 109-071.
- c. There is a similar requirement for states to have a security plan in order to qualify for the automatic grant allocation minimum in S. 1013 and S. 21.
- d. H.R. 1 states "each of the States, other than Virgin Islands, American Samoa, Guam and the Northern Mariana Islands..."
- e. "Additional high-risk qualifying criteria consists of - (A) having a significant international land border; or (B) adjoining a body of water within North America through which an international boundary line extends." H.R. 1, Implementing the 9/11 Commission Recommendations Act of 2007, Sec. 2004-6.
- f. S. 1013, Sec. 1802, A, I, May 12, 2005.