



Strategies and Methods for Informing Risk Management: An Alternative Perspective

A White Paper

6 September 2011



HOMELAND SECURITY
STUDIES AND ANALYSIS INSTITUTE

An FFRDC operated by Analytic Services Inc. on behalf of DHS
2900 South Quincy Street • Suite 800
Arlington, VA 22206-2233

Prepared for the
Department of Homeland Security
Directorate of Science and Technology

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the “Act,” authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. Analytic Services Inc. operates the Homeland Security Studies and Analysis Institute as a FFRDC for DHS under contract HSHQDC-09-D-00003.

The Institute provides the government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing evaluation in tandem with the government’s acquisition process. The Institute also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise.

The Institute’s research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under

Task 09-01.00, Strategies and Methods for Informing Risk Management (Core Allotment)

The purpose of the task is to develop recommendations for how the DHS Science and Technology Directorate and the department might feasibly improve and implement risk assessments and make risk management decisions.

The results presented in this report do not necessarily reflect official DHS opinion or policy.



An FFRDC operated by Analytic Services Inc. on behalf of DHS

TASK LEAD

David McIntyre, PhD
Distinguished Visiting Fellow

TASK TEAM

Wallace Langbehn
Manager,
Threats and Risk Analysis Division
Mark Hanson
Manager,
Operations Analysis Division
Steven Chabolla,
Principal Analyst

STRATEGIES AND METHODS FOR INFORMING RISK MANAGEMENT: AN ALTERNATIVE PERSPECTIVE

A White Paper

6 September 2011

Prepared for
Department of Homeland Security
Directorate of Science and Technology

ACKNOWLEDGEMENTS

Special thanks are due to Mr. Bob Ross,
Department of Homeland Security, and
Dr. Mark Gallagher,
Department of the U.S. Air Force,
for sharing their own extensive scholarly work in this field.

For information about this publication or other Institute research, contact

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

Analytic Services Incorporated
2900 S. Quincy Street
Arlington, VA 22206
Tel (703) 416-3550 • Fax (703) 416-3530
www.homelandsecurity.org

Publication Number: RP09-01.00-18

As part of the Institute's charter to provide independent analysis of homeland security issues for DHS, this document is part of a series intended to present thought provoking ideas and considerations on proposed topics of interest. This study is a result of a request from the DHS Science and Technology Directorate for the Institute to assess the approaches and methods used by DHS for informing risk management decisions, with the goal of offering fresh perspectives.

Dr. David H. McIntyre, a Distinguished Visiting Fellow with the Homeland Security Studies and Analysis Institute, provides this fresh look perspective. He is a nationally recognized strategist, analyst, teacher, and lecturer with over 24 years specializing in national and homeland security issues. Dr. McIntyre served on numerous national level blue ribbon committees, to include appointment to the National Security Education Board by President Bush in June 2008. Dr. McIntyre is also the former director of the Integrative Center for Homeland Security at Texas A&M University.

The research and analysis presented here is intended to provide unique perspectives on key homeland security issues. While this effort was conducted under the auspices of the Homeland Security Studies and Analysis Institute, the results and opinions do not necessarily reflect those of the Institute or the Department of Homeland Security.

This page intentionally left blank

TABLE OF CONTENTS

Executive Summary	1
The Task.....	3
<i>Scope and Goals</i>	3
<i>Methodology</i>	4
Summary of Observations and Recommendations.....	5
<i>Observations</i>	5
<i>Recommendations</i>	6
Background: DHS and Risk	7
National Risk Assessment.....	12
Observations: Calculating & Prioritizing All Risk to Everything	13
Recommendations: Rethinking a National Risk Assessment.....	15
The Language and Communication of Risk in DHS	19
Observations: The Terminology of Risk in DHS is Problematic	19
<i>The Language of Risk</i>	19
<i>The Communication of Risk</i>	23
Recommendations: Rethinking the Language and Communication of Risk in DHS.....	25
<i>Change the Concept and Language</i>	25
<i>Communicate Risk Reduction in a Positive Way</i>	25
Practicing Risk Thinking.....	27
Observations: On Risk-Informed Decision Making.....	27
<i>Some Warnings from the Past</i>	27
<i>Better Understanding through Risk Typology</i>	29
<i>Dynamic Risks</i>	30
Recommendations: Explaining Better the Risk of Risk	36
<i>Visualize Risk Information</i>	36
<i>Conceptualize Risk Operations</i>	39
Advancing Risk Management in DHS	43
Observations: On the Progress of Risk Efforts in DHS.....	43
Recommendations: Advancing the Risk Endeavor in DHS	45
The Culture of Risk Management.....	49
Observations: On the Problem of Establishing a Risk Management Culture.....	49
Recommendations: Some Ways to Promote a Culture of Risk Management	50
<i>Establish a Sense of Urgency</i>	51
<i>Create a Guiding Coalition</i>	51
<i>Develop a Vision and Strategy</i>	51
<i>Communicate the Vision and the Change Required</i>	52
<i>Give People in the System the Power to Make the Changes Work</i>	52
<i>Plan for Some Short-Term Wins</i>	52
<i>Leverage These Gains to Encourage More Change</i>	52
<i>Anchor the Changes Into the Long-Term Culture</i>	52
Final Thoughts.....	55
Appendix A – Key Definitions.....	57
Appendix B – The Deming Method	59
The Fourteen Points	59
The Seven Deadly Diseases	59

Appendix C – Reasons People Oppose Change60
Appendix D – Comments From Interviews And Reviews.....63

EXECUTIVE SUMMARY

For a decade, parties inside and outside the Department of Homeland Security (DHS) have been encouraging the development and use of common risk management approaches in the field of homeland security. Despite the serious efforts of many dedicated individuals, the promise of a unified approach that reduces risks, maximizes effects across the enterprise, and minimizes costs, has not been realized. As the executive agent for the Homeland Security Studies and Analysis Institute (the Institute), the DHS Science and Technology Directorate asked the author to research integrated risk management and use his professional background in national strategy and government operations to develop insights into the subject.

Research for this paper led to five fundamental messages:

- The Department of Homeland Security as a whole and a number of subordinate agencies in particular, are doing a laudable job of creating and applying risk management tools and concepts to inform future department decisions, policies, operations, and acquisitions. But the effort as currently conceived will fall short of expectations because the task of calculating national risk by starting with all potential threats and evaluating them against all potential targets, vulnerabilities, and consequences is simply too big to manage.
- A better approach is to identify the maximum possible events we might face, then use the techniques of risk management to evaluate and prioritize them—under the theory that by preparing for the “maximums of maximums” (a new FEMA approach), we also prepare for lesser challenges to homeland security. This approach could lead to an achievable national-level homeland security risk assessment.
- Additionally, the entire risk effort could benefit from a major change to the language of risk, emphasizing the positive goal of improving safety and security, rather than the negative goal of reducing risk.
- The current approach to integrated risk management promotes the oversimplification of information to make the task of decision makers easier. But this could lead to overconfidence and blindness to important aspects of each unique situation. Disaggregating risk analysis to offer additional presentation tools might help decision makers grappling with this challenge.
- Calculating and presenting risk correctly is a complex matter. Advancing risk management enterprise-wide would benefit from the establishment of a separate risk career field.

A number of pragmatic steps, ranging from improving training and education to a focused attempt to change the homeland security culture’s acceptance of risk management, can and should be undertaken. The Origin of this Study

Risk, risk assessment, risk analysis, and risk management are terms long associated with the fields of insurance, economics, and finance, and have made their way into many

fields of private and public endeavor, from engineering and medicine to education and security.¹ Since 9/11 there has been an especially strong push at the federal level (from both U.S. Congress and two presidential administrations) to apply these concepts to the problem of homeland security.

The Department of Homeland Security continues to advocate risk management principles and the development of processes toward those principles. Congress, moreover, continues to expect improvement and results regarding the department's use of risk in its decision making. Accordingly, the Homeland Security Studies and Analysis Institute asked the author to research and prepare a white paper on the subject of "Strategic Approach and Methods for Informing Risk Management."

In particular, in its proposed act to authorize 2011-2012 appropriations for the Directorate of Science and Technology (H.R. 4842), Congress sought to levy specific risk management and assessment requirements on the Secretary of Homeland Security.² Although oriented primarily toward informing science and technology investments, if passed, the act will require a national-level risk assessment, which departments can then use to assess risk in their planning, programming, budgeting, and operations. The U.S. Congress did not pass the bill as drafted—the session ended, during the research and writing of this paper, without the enactment of H.R. 4842. However, their expectations as outlined in the bill's language will likely endure.³

But, the homeland security community has not been able to attain the long desired goal of a national-level homeland security risk assessment despite the best efforts of some talented and hard working public servants. Further, risk management

- remains a foreign and confusing language for many in the national enterprise of homeland security;
- is not relied upon routinely to inform decision makers about homeland security issues;
- has not gained the momentum required to really impact the entire Department of Homeland Security and the rest of homeland security's national enterprise; and
- is far from achieving its desired place in the culture of the department.

In asking "Why?" these assessments are so, this white paper applies a new perspective—that of an experienced strategist rather than an expert risk manager. This paper also asks "How?" regarding what to do about this situation. As a result, this paper offers some recommendations about how to use risk management (and all the additional risk work at

¹ One of the problems of this field is that different communities in it use different definitions of key terms. Appendix A contains the currently approved DHS definitions for these terms.

² This refers to H.R. 4842, 111th Cong. (2002).

³ A full text of the draft bill is available at <http://www.govtrack.us/congress/bill.xpd?bill=h111-4842>.

DHS that is ongoing and worthwhile) as a valuable means to the end of improved safety and security for the nation.

The Task

During that last session of the U.S. Congress, the U. S. President signed Presidential Policy Directive (PPD) 8, a directive animated by the same spirit as H.R. 4842 regarding the adoption of risk management as a guiding principle for DHS. The directive included setting priorities for the department's planning, programming, budgeting, and operations. Consequently, the author modified the research and writing during this study to include the ways in which PPD-8 offers the same challenges and opportunities for DHS risk management that H.R. 4842 does.

Cognizant of H.R. 4842, and recognizing that the department continues its struggle with finding an implementable risk management approach, the Institute's executive agent affirmed the Institute's original idea for this study by requesting to see the study upon its completion.

Scope and Goals

Using the context of H.R. 4842 and existing DHS risk management and assessment practices, this paper takes a fresh look at how DHS might improve risk management, including risk assessments. Despite a number of past and current efforts in developing approaches to homeland security risk management and assessment, no current department-wide approach has matured to a level of acceptance for informing routine DHS decision making. The limitations of these past approaches, including the level of detail, resource requirements, and time required to perform the activity, have delayed implementation. By applying fresh thinking, this study attempts to contribute to the solution of this enduring problem.

The scope of this study was research addressing the strategic, operational, and tactical needs of risk managers, and the requirements of their risk assessments. The author also considered the impact of current risk management practices within the department. Rather than develop specific risk models or techniques, this study concludes with broad recommendations that could improve the Department of Homeland Security's use of risk assessments in decision making.

The goals for this study, as the Institute stated in the task order, were to

- develop recommendations for how the Department of Homeland Security might feasibly implement risk assessments and make risk management decisions within the context of H.R. 4842's requirements, and
- provide a new perspective—that of a strategist—on an enduring problem.

Methodology

The research for this study included the following, explained in further detail below.

- A focused literature review.
- Attendance at eight risk-related events (conferences, presentations, etc.).
- Informal interviews with more than two dozen people who have worked within the senior ranks of homeland security and within the risk management field.
- The author focused the literature review primarily on government documents to determine the intent and direction of risk-related developments within DHS over time. The chronological development of reviews, concepts, and organizations is important to show the extensive work already completed in this field—and the attendant frustration. As it became clear that DHS conceives risk management differently from other parts of homeland security’s national enterprise, the literature review expanded to the areas of economics, banking, and finance.

The risk-related conferences and other events included several that were *not* focused on risk management alone, but that offered the opportunity to query participants about their understanding and use of risk concepts.⁴ The participants included a former Secretary of Homeland Security, intelligence experts, educators, business people, and several local emergency responders. These presentations and sessions helped redirect the research and other interviews. The events also gave the author a better understanding of how poorly risk management is understood or used outside the community of risk managers.

Numerous current or previous government employees, with a wide range of risk and homeland security expertise, generously consented to confidential interviews on this subject, leading to observations that could have filled a report several times this long.⁵ Notes from these meetings were transcribed, color coded by topic, and methodically compared to create the observations enclosed. Comments on accuracy and clarity were addressed in the paper’s editing process. While the perspectives were different, the visions they related were strikingly consistent. Nearly every person interviewed for this report saw risk management as an important endeavor that has matured significantly. But most found the analytic tools too primitive, the trained workforce too small, the data too thin, and the expectations for precision too great to satisfy nationally expressed

⁴ These conferences included: “NDIA 2010 Homeland Security Symposium and Exhibition, 09/28/2010 - 09/29/2010, Washington, DC.; “Consortium for Homeland Defense and Security’s Fifth Annual Symposium,” 16 November 2010, Washington, DC; “*Center for Homeland Defense and Security* Continental Security Workshop,” December 07-08, 2010, Colorado Springs, Colorado; Intelligence Specialists, Command & General Class College, Ft Leavenworth, KS, 17 January, 2011; “5th Annual Homeland Defense and Security Education Summit,” sponsored by Homeland Security and Defense Education Consortium Association, 10 March, 2010, College Park, Maryland; and others .

⁵ As agreed during interviews, all names have been withheld.

expectations any time soon. Some comments either addressed issues outside the scope of this paper, or disagreed with conclusions. Those comments that seemed especially instructive have been included at the end of the paper in Appendix D.

In the final step of the development of this white paper, the author analyzed these findings based on his 20 years experience writing, teaching, and practicing strategy at the national level. This analysis generated the following questions which prompted several new insights:

- What different outcome might DHS achieve with the tools at hand? This led to new thinking not only about the national risk assessment that H.R. 4842 and PPD-8 require, but also about the use of that assessment to inform science and technology and other departmental priorities.
- Why is DHS struggling with those tools? This led to new thinking about the language of risk and the presentation of risk to decision makers.
- How might DHS advance the use of risk assessments and the acceptance of risk management within the department? This led to new thinking about how to advance risk efforts further in DHS and how to integrate risk management into the departmental culture.

Summary of Observations and Recommendations

Research for this paper led to observations and corresponding recommendations in five major areas. Explained in the forthcoming sections of this paper, they are summarized as follows.

Observations

1. *From a strategic perspective, even where it is being applied, risk management is not working as desired in the field of homeland security.* It is not providing an agreed upon philosophical approach, compatible across the national enterprise of homeland security for the nation, that can be used to establish priorities ranging from the national level (e.g., a national risk assessment), to the departmental level (e.g., allocation of resources in science and technology), to the local level (e.g., a grant proposal or preparedness plan).
2. *The discussion of risk and of risk assessment is undermined by the language it has inherited from banking, insurance, finance, and other fields.* A change in terminology to focus on national safety and security, rather than risk management, would solve this problem.
3. *Properly conducting risk assessments is not enough.* DHS must effectively convey both the risks and limits of analyst knowledge and related uncertainties, to decision makers.
4. *Risk concepts have still not been broadly accepted and applied across homeland security's national enterprise.*

5. Promoting risk management as “the way we do business” requires the *establishment of a “risk management culture” within the department.*

Recommendations

1. *Address the largest dangers first, regardless of likelihood.* That is a strategic alternative to the current complex approach to considering all risks. The theory behind that approach is that preparing for a larger danger will improve preparedness for smaller, if not more likely dangers. Once the large dangers—those likely to produce the worst consequences—are identified, a risk analysis of just those threats will allow us to focus first on the most dangerous combinations of threats, vulnerabilities, and consequences. The result would be a National Threat Assessment focused on what the Federal Emergency Management Agency (FEMA) calls the “maximum of maximums.”
2. *Change the language, replacing “risk” with a concept and body of terms and processes that DHS can own from the outset and focus on the homeland security mission.* Communicate this concept in a clear, positive way. For example, instead of stressing “risk reduction,” talk about “improving safety and security.”
3. *Include the following three new initiatives in risk management:*
 - Create new tools for visualizing and explaining risk assessment and analysis.
 - Adopt the new concept of “risk severity,” which includes the cost of addressing risk.
 - Consider how to promote the active daily “management of risk” in addition to the already accepted “risk management.”
4. *Establish risk management skills and professionals within DHS,* to expand the thinking about and impact of risk within the department and the rest of homeland security’s national enterprise.
5. *Develop a risk management culture at DHS* by applying some of the best, most recognized research techniques. Such transformations have been the subject of considerable modern research and DHS could benefit from that research.

BACKGROUND: DHS AND RISK

For nearly a decade, the role of risk in the federal approach to homeland security has been growing in formality and importance.

Well before 9/11 and as long as two years before the Department of Homeland Security was created, experts from the Government Accountability Office (GAO) and elsewhere began to speculate that risk management would be an important organizing principle for U.S. homeland security efforts.⁶ Only ten days after 9/11 the GAO called specifically for a national risk assessment:

The United States does not have a national threat and risk assessment to help guide federal programs for homeland security. A threat and risk assessment is a decision-making tool that helps to define the threats, to evaluate the associated risk, and to link requirements to program investments. In our March 2001 testimony on combating terrorism, we stated that an important first step in developing a strategy for combating terrorism is to conduct a national threat and risk assessment to define and prioritize requirements.... Combating terrorism is a major component of homeland security, but it is not the only one. It is essential that a national threat and risk assessment be undertaken that will address the full range of threats to the homeland.⁷

The Homeland Security Act of 2002 and the formation of the department in 2003 reflected a growing congressional interest in risk assessment.⁸ When the Office of Domestic Preparedness was transferred from the Department of Justice to DHS in 2003, it brought with it a risk-based grant process for state and local governments.

The report of the 9/11 Commission, released in July 2004, recommended that the process and calculation of risk analysis (which had been based primarily on population) be revised.⁹ The first of several changes to the formula for calculating risk followed.

Then Secretary of Homeland Security Michael Chertoff established risk management as the “core principal” of DHS activity as part of his Second-Stage Review in 2005.¹⁰ In

⁶ General Accountability Office (GAO), *Comments on Counterterrorism, Leadership, and National Strategy*, GAO-01-556T, (Washington, DC: GAO, March 27, 2001); _____, *Homeland Security: Key Elements of a Risk Managed Approach*, GAO-02-150, (Washington, DC: GAO, October 12, 2001); _____, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T, (Washington, DC: GAO, October 31, 2001).

⁷ GAO, *Homeland Security: A Framework for Addressing the Nation’s Efforts*, GAO-01-1158T, (Washington, DC: GAO, September 21, 2001).

⁸ Homeland Security Act 2002, Public Law 107-296, 107th Cong., (2002), http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.

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

contrast to others who have pushed risk management primarily as a way to prioritize and manage budgets and funding, Secretary Chertoff also saw it as a way to rethink the organization and functions of the department. He noted pointedly:

Old categories, old jurisdictions, old turf will not define our objectives or the measure of our achievements. Because bureaucratic structures and categories exist to serve our mission, not to drive it. What should drive our policies and operations and the way we are organized is this strategic matrix of threat, vulnerability and consequences. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.¹¹

As part of Secretary Chertoff's efforts, the formula for risk analysis was modified to its present form (Risk = Threat x Vulnerability x Consequences, or $R = T \times V \times C$).¹²

That same year, in 2005, the GAO issued a report that finalized a risk management framework that became the prototype of the framework that DHS uses today. The new structure "synthesized information from numerous government, industry, and academic sources" reaching back to 1993.¹³ Appendix I of that report explained the framework and included a first-of-its-kind glossary of risk management as it applied to DHS.

In 2007, the Congressional Research Service issued a report containing a comprehensive description of the evolution of risk assessment and risk management in DHS, as well as major issues raised, and some options for congressional intervention.¹⁴

In 2008, the GAO convened a forum to collect and publish effective public and private sector risk management practices.¹⁵ That same year DHS issued its first version of a

¹⁰ Christopher Cox (Chairman) et al., *The Secretary's Second-Stage Review: Re-thinking The Department Of Homeland Security's Organization and Policy Direction Parts I And II: Hearing Before the House Committee on Homeland Security, House of Representatives, One Hundred Ninth Congress, First Session, Serial No. 109-32* (Washington, DC: U.S. House of Representatives, July 14, 2005), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:27687.pdf. This is perhaps the best available single document explaining the Second-Stage Review. In this testimony, Secretary Chertoff explains the review, its purpose and outcome, and his anticipated changes to DHS. The House Committee on Homeland Security provides opening comments on the subject, and follow-on questions and answers are provided. Secretary Chertoff's explanation begins on page 7.

¹¹ "Chertoff Outlines Risk-Based Strategy for Long-Term Homeland Security," *Continuity Central*, 17 March 2005, <http://www.continuitycentral.com/news01794.htm>.

¹² Some specialists point out that risk is really a function of the relationship between T, V, and C, and not necessarily a multiplicative product. Nevertheless, the most recent FEMA training aimed at a general audience (on line at learnaboutrisk.org) treats the relationship as a straight calculation: $R = T \times V \times C$.

¹³ GAO, "Appendix I: Risk Management Framework," *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91, (Washington, DC: GAO, December 2005), 100-112.

¹⁴ Todd Masse, Siobhan O'Neil, and John Rollins, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, RL33858 (Washington, DC: Congressional Research Service, February 2, 2007).

lexicon for risk management—the first of many documents by which the Director of the Office of Risk Management and Analysis sought to provide central direction to DHS on this issue.¹⁶

In 2009, the revised National Infrastructure Protection Plan devoted an entire chapter to how it would be informed by risk.¹⁷

That same year DHS also issued a formal Integrated Risk Management Framework.¹⁸ The structure and content of this framework (especially the risk management cycle on page 8) bears a strong resemblance to the framework that the GAO previously issued. One significant addition was the inclusion of risk communication in every phase of risk management.

A major development in the history of risk management at DHS was the release of the *Quadrennial Homeland Security Review* in 2010. The report is noteworthy because it identifies a national-level homeland security risk assessment as a major step required to move forward toward “Maturing and Strengthening the Homeland Security Enterprise.”¹⁹

Also in 2010, the Secretary of Homeland Security issued a memorandum entitled “DHS Policy for Integrated Risk Management.” This document formalized a number of organizational aspects of the DHS risk effort. It included assigning lead responsibility to the National Protection and Programs Directorate and coordination authority to the Director of Risk Management and Analysis, and establishing a number of coordinating committees and processes.²⁰

Finally, in 2010, DHS released an updated *Risk Lexicon*, the Risk Management Curriculum Review Group published an educational report, and various organizations within DHS refined multiple tools for risk management.²¹ Additionally, as noted above,

¹⁵ GAO, *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-904T, (Washington, DC: GAO, June 25, 2008).

¹⁶ Risk Steering Committee, *DHS Risk Lexicon, 2008 Edition* (Washington, DC: Department of Homeland Security, 2008).

¹⁷ Department of Homeland Security, “Chapter 3: The Strategy: Managing Risk,” *National Infrastructure Protection Plan* (2009).

¹⁸ Risk Steering Committee, *Interim Integrated Risk Management Framework* (Washington, DC: Department of Homeland Security, January 2009).

¹⁹ Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (February 2010), 66.

²⁰ Janet Napolitano, “DHS Policy for Integrated Risk Management,” memorandum, May 27, 2010. (FOUO)

²¹ Risk Steering Committee, *DHS Risk Lexicon, 2010 Edition*, (Washington, DC: Department of Homeland Security, September, 2010); George Tanner et al., *Risk Management Curriculum Review Group: Findings Report* (Washington, DC: Department of Homeland Security, December 2010); Because this study was directed to *not* review or examine the tools and programs actually used to analyze risk, those artifacts are not included in the history given here. However, several such tools have been developed to identify and calculate risk. The *Maritime*

H.R. 4842 was also introduced, proposing the establishment of a national risk assessment and directing that DHS plans, programs, budgets, operations, etc., be aligned with the results.

In early 2011, a major step forward in establishing a comprehensive homeland security risk management doctrine was achieved with the Department of Homeland Security's release of the capstone document *Risk Management Fundamentals*.²² Outlining objectives, tenets, and principles, this represents the first of an anticipated series of publications intended to "provide a structured approach for the distribution and employment of risk information and analysis efforts across the department."²³ One month later, an expanded DHS directive replaced the 2010 policy memorandum for integrated risk management, thereby formally establishing the structure of and responsibility for the DHS risk effort.²⁴

In March 2011 President Obama released PPD-8 (National Preparedness), which specified that the new national preparedness goal, due by September 30, 2011, "shall be informed by the risk of specific threats and vulnerabilities—taking into account regional variations—and include concrete, measurable, and prioritized objectives to mitigate that risk."²⁵

Risk informed decision making is clearly intended to be a major catalyst in shaping the strategy, policy, operations, plans and funding of DHS. Many organizations within DHS are implementing risk management programs and strategies, ranging from operators in the Transportation Security Administration (TSA) to researchers in the Directorate of Science and Technology. FEMA offers training in the subject, and multiple approaches to calculating risk are now available from the Coast Guard and other government agencies and contractors. However, no one has yet established an acceptable way of combining all these efforts to produce a National Risk Assessment.

Security Risk Analysis Model deserves special notice, since it has repeatedly been praised by outside evaluators for its utility in improving port and maritime security at the tactical level. Meanwhile, the Homeland Security Studies and Analysis Institute began developing the *Risk Assessment Process for Informed Decision-Making (RAPID)*, which has been used successfully at the strategic level. No single tool has been developed to address all types and levels of risk.

²² National Protection and Programs Directorate, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, DC: Department of Homeland Security, March 2011).

²³ *Ibid*, 1.

²⁴ DHS, Directive 007-03, "Integrated Risk Management," (Washington, DC: Department of Homeland Security, March 28, 2011).

²⁵ Presidential Policy Directive (PPD-8), "National Preparedness," March 30, 2011. Note: "This directive replaces Homeland Security Presidential Directive (HSPD)-8 (National Preparedness) issued December 17, 2003, and HSPD-8 Annex I (National Planning), issued December 4, 2007, which are hereby rescinded."

Despite this lack of consensus, however, PPD-8 and the pending National Preparedness Plan now require a national risk assessment. It is likely that future directives and legislation will require that the national risk assessment be applied to other parts of the Department of Homeland Security as well, much as the proposed H.R. 4842 stands to demand of the Science and Technology Directorate.

The next section details an observation—and offers to DHS a recommendation—about the impending national risk assessment.

This page intentionally left blank

NATIONAL RISK ASSESSMENT

From a strategic perspective, the concept of risk management is not yet working as intended in the field of homeland security. It is not providing an agreed upon philosophical approach, compatible across the national enterprise for homeland security, that can be used to establish priorities ranging from the national level (as in a national risk assessment), to the departmental level (as with the allocation of resources in the Science and Technology Directorate), to the local level (as in a grant proposal or preparedness plan). Evidence includes the struggle for uniformity in the application of risk within DHS, the difficulty in producing the national risk assessment long desired by senior leaders and demanded by the U.S. Congress, and the reluctance of participants across the homeland security enterprise to embrace risk-based activities. Thus, despite the discipline of a decade-long requirement, the federal practitioners of risk management have not been able to produce a national risk assessment, to routinely inform planning, programming, or budgeting. As noted above, U.S. Congress responded to this situation by drafting H.R. 4842 in 2010.

Observations: Calculating & Prioritizing All Risk to Everything

Risk management's struggle for acceptance is somewhat surprising, since risk assessment, risk analysis, and risk management do work well when there is a simple, direct cause-and-effect relationship between threat-input and consequence-outcome. In fact, risk analysis is in many respects simply the reverse of the sophisticated targeting approach called *effects-based operations*, which the U.S. Air Force champions.²⁶ In that strategy, the focus of the military and its related resources is on achieving the desired effect from the enemy, rather than on simply identifying and destroying categories of targets. If the concept works for targeting and attack, it would seem to make sense that they would work in reverse for prevention and protection—that is, to identify those things that an enemy might target to produce an effect in our nation, so that we might prevent such attacks. The application of risk to homeland security actually springs directly from the effort to identify, prevent, or mitigate terrorist attacks.

Calculating risk when an enemy might attack targets across the entire economic, social, or political enterprise of a nation is difficult. It is not like calculating risk when considering an attack on a single target, functional area, critical infrastructure (e.g., power plant), or key resource (e.g., food distribution company); that calculation, like the

²⁶ The Air Force argument in support of Effects Based Operations (EBO), a variation of traditional military strategy, has been evolving since at least the Gulf War of 1990. While hundreds of articles and explanations are available from reliable sources, there is no single best source. The debate over how to select and produce the right effect—and, indeed, over whether this really represents a new approach to strategy—continues. The important point to understand is that EBO focuses on creating a cascade of powerful effects by attacking the enemy—precisely what we attempt to identify in thinking how an enemy might do that to us, and to prevent that through a risk informed defense.

mitigation of that risk, is relatively straightforward. That single-target type of attack can be likened to a military attack of known size and type; figuring the wartime consequences of that is straightforward.

Put another way, figuring the strategic, operational, planning and budgetary implications of a doctrinal attack is much simpler than calculating the risk to thousands of targets exposed to dozens of terrorist attack venues. The latter is especially difficult when little hard data about the enemy is available. At some point, the uncertainties and complexities of estimating risk mount to the point that the utility of the entire risk assessment effort becomes doubtful. This is especially the case where the bench of trained quantitative experts across the homeland security enterprise is thin.

Despite the best efforts of good people, risk management of every potential target across the entire national enterprise of homeland security will never provide the strategic starting point for informed decision making that Congress is searching for with H.R. 4842.

Essentially, this approach by Congress to risk management, with H.R. 4842, would use our limited resources to make incremental improvements to the defense of a large number of potential targets, marginally reducing a nearly infinite list of potential attack vectors mounted by an adaptive enemy. The H.R. 4842 approach would try to reduce the most dangerous outputs (consequences) by guessing and preempting all the inputs (threats and vulnerabilities). Meanwhile, an adaptive opponent can focus on just a few inputs while seeking to create newer and cheaper lines of attack at the same time. Even under the best of circumstances, we are not likely to win this game.

Thus the core problem of the national risk assessment is that what is most logical in concept is not feasible in practice. Creating a traditional, bottom-up national risk assessment from scratch would require the production of thousands of databases and risk analyses—more than DHS can create and manage, and more than most jurisdictions are trained or willing to produce. FEMA training (<http://www.learnaboutrisk.com>) recommends that every jurisdiction begin with analysis of about 300 potential targets. The well known imprecision of the term “jurisdiction” combined with a widely accepted estimate of 80,000 jurisdictions nationwide means a national risk assessment would include 24,000,000 points of interest. Several years ago, public and private enterprise members balked when asked just to submit much simpler lists of their critical infrastructure and key resources (CI/KR).²⁷ Consequently, it is not reasonable to believe that complex calculations on this scale will be accomplished by inexperienced local personnel, or a handful of people working at the national level.

Additionally, it is not reasonable to expect that the intelligence community could generate threat estimates for hundreds of targets in each of thousands of jurisdictions,

²⁷ This general reluctance of responsible parties to share CI/KR data is a well known challenge confirmed by several experts during private interviews. A concerted effort by DHS over time to promote cooperation through Information Sharing and Analysis Centers and other forums has produced progress but not a solution.

even if it called on the new system of state and local intelligence fusion centers. And should those jurisdictions submit a quarter million risk analyses to DHS, the department would have no agreed upon standard to judge the many different nominations, all produced by different approaches to risk analysis. The current approach to risk management does not mandate a single process for analysis, but instead encourages organizations to select their own tools and approaches to the actual calculations.

Beyond these practical issues, the U.S. Congress and the current presidential administration have been seeking to use risk in a broader way to improve the quality of senior leader decisions. Their work indicates that a national risk assessment should inform not just the funding of grants for target protection, but the development of plans and policies, the creation of budgets, and even research and the purchase of technologies. But a national risk assessment that attempts to evaluate and compare every possible terrorist threat, using every means of attack, against the vulnerabilities of every potential target and the consequences of every possible combination (while allowing the originating jurisdictions to use their own standards in the evaluations), would overwhelm decision makers as well as analysts. What decision makers want from risk management is small clear numbers. What the logic of the current system produces is large opaque numbers.

This conundrum dictates that we find a way to focus our risk management efforts on a manageable number of assets even before we begin the process of actual assessment and analysis. Perhaps finding a way to focus on some threats over others would help.

Recommendations: Rethinking a National Risk Assessment

The goal of the national risk assessment is to identify those “threats that pose the greatest risk to the security of the Nation.”²⁸ But, as observed above, calculating and comparing every risk from every threat is not practical.

A strategic alternative is to start by addressing the greatest potential consequence first, under the theory that preparation for “such maximum” events will improve preparedness for smaller but more likely dangers as well. Once the maximum concerns are identified, we can focus on a risk analysis of just those specific combinations of threats, vulnerabilities, and consequences most likely to produce the greatest dangers.

The result would be a national threat assessment not focused on every terrorist threat, but on the worse possible events—what FEMA calls the “maximum of maximums.”²⁹

So a national risk assessment might proceed as follows: DHS would begin by agreeing on a list of national maximum of maximums. FEMA has already begun this process with the

²⁸ PPD-8, 5.

²⁹ Since 2009 FEMA has been preparing for catastrophic events by using the *maximum of maximums* approach, which focuses on developing capabilities to stabilize a major all-hazards event within 72 hours, complete initial recover in 60 days, and fully recovery within five years. The major change from the past is to elevate the scale of events for focus, discussion, and preparation.

intent of replacing the “15 national scenarios” presently used to identify required capabilities for addressing homeland security concerns, with events more likely to stress the nation as a whole.³⁰ The logic is familiar, as follows:

- If we prepare for a large Mumbai style ground attack, we will be better prepared for the more likely lone gunman.
- If we prepare for a large pandemic, then we will be better prepared for smaller, more localized disease outbreaks.
- If we prepare for a large-scale destructive event (like an earthquake in an entire region), then we will be better prepared for an improvised explosive device (IED) at a local sporting event.³¹

Homeland security workers are familiar with the all-hazards approach. Think of this as the all-maximum events approach.

DHS would then tie future state, local, and business grants to those combinations of threat, vulnerability, and consequence that could produce a maximum-of-maximums event.³²

These combinations would be collected at the FEMA regional level, and be called *regional maximum risks*. (Obviously, this list would be built with state and local input.) With assistance from FEMA Headquarters as required, FEMA regional staffs would conduct a risk analysis of what they identify as the regional maximum risks. DHS would field a risk analysis/risk management team to each region to provide assistance and to standardize this process. As always, this process must be transparent, with major stakeholders represented in the deliberations.

After prioritizing the regional maximum risks, each region would conduct an analysis of the gap between needs and capabilities available to address this list, assuming the use of existing resources from the entire community (a “whole of community” capability gap analysis). These needs should include both short-term resources and longer-term research

³⁰ Before the shift of FEMA’s focus to maximum of maximums, homeland security capabilities were created and evaluated against a list of 15 potential scenarios, ranging from natural disasters to nuclear or biological attack. Like the maximum of maximums, these scenarios were *not* selected because they were likely to take place, but because they required the development of a broad range of responses which could be evaluated for preparedness.

³¹ During interviews for this paper, several knowledgeable people expressed concern over the maximum-of-maximums approach. They were concerned that just as preparing for a large mechanized war did not prepare DOD for fighting terrorists in Afghanistan, preparing for the maximum of maximums might not create capabilities for lesser included events. Mechanized warfare and counterterrorism are quite different, and of course concentration on preparation for one would *not* create forces simultaneously prepared for the other. But this objection is not born out with the maximum of maximums where each “maximum” event differs from lesser included events only in scale.

³² Obviously, this list of maximum of maximums would not be perfect. The criterion for “maximum” selection would be refined with every evaluation cycle.

and development requirements. Those requirements would be forwarded to the DHS Science and Technology Directorate to promote risk informed prioritization of projects. This would also help the directorate satisfy H.R. 4842, should U.S. Congress end up passing the resolution.

Based on the regional maximum risk analysis and community capability gap analysis, each FEMA regional director would make a recommendation to DHS for funding distribution within his or her region. DHS would validate the prioritized list within each region. To provide an incentive for enterprise-wide cooperation, local and regional funding requests that showed whole of community cooperation across and between regions would receive special consideration.

DHS staff would then compare and prioritize between regions to identify national maximum risks—a task that could reasonably be assigned to the National Infrastructure Protection Plan. The prioritized list of national maximum risks would become the national risk assessment. Such an assessment would, by its nature, inform the creation of the national preparedness goal that PPD-8 requires, including the “core capabilities necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the nation.”³³ It would also satisfy the intent of draft H.R. 4842. And because the process would begin by asking local, state, and then regional participants to manage their maximum-of-maximum risks, it would promote the “integrated, layered, and all-of-nation preparedness approach that optimizes the use of available resources,” as PPD-8 directs.³⁴

Thus the national risk assessment should not be an integrated list of millions of targets that would assign regions into a rank order for grants. Instead, the process of producing the national risk assessment would deliver to DHS the following:

- A list of the biggest maximum-of-maximums events by category;
- A list of potential maximum-of-maximums events from each region called a regional maximum risk;
- A regional risk analysis of the events producing maximum-of-maximums events;
- A layered capability gap analysis of each region’s ability to respond to its regional risk analysis;
- A list of research and development needs based on maximum-of-maximums events and otherwise informed by risk, and
- A consolidated list of all this information that would identify the national maximum risk, plus the prioritized list of risk calculations that would constitute the national risk assessment.

³³ PPD-8, 2.

³⁴ *Ibid.*, 2.

The effect of this approach is to integrate the national risk assessment with the National Preparedness System at every step. In accordance with the doctrine established by the *Framework for Risk Management*, the assessment would be repeated periodically.³⁵

As will be discussed later, aggressive communication of risk across the entire national enterprise of homeland security would be essential to this focused approach. If DHS were able to take this approach, the objection might be raised that DHS was accepting “low-consequence” risk or abandoning some people and targets in favor of others. Other critics would note that some small events might unexpectedly cascade into maximum-of-maximums events. DHS would have to argue that perfect protection of everything everywhere against all threats and hazards is both impossible and economically impractical. The best way to protect all people and all assets in the United States is to focus on the national maximum risk, and to use that process to identify lesser risks that other elements of the national enterprise of homeland security would address.

³⁵ For general readers, the National Preparedness System is the organizational construct that collects the elements of the National Preparedness Guidelines (Capabilities Based Preparedness, national Planning Scenarios, Target Capabilities List, Universal Task List), under a common framework with Preparedness Policy and Doctrine, Planning and Resource Allocation, Training, Exercises & Lessons Learned, and Assessment and Reporting. According to *National Preparedness Guidelines*, Washington, DC: Department of Homeland Security, September 2007 (p.22), this system “provides opportunities for all levels of government, the private sector, nongovernmental organizations and individual citizens to work together to achieve proprieties and capabilities outlined in the Guidelines. An official National Risk Assessment could be integrated into every aspect of the preparedness system, providing the “information environment” in which all preparedness activities were pursued at every level.

THE LANGUAGE AND COMMUNICATION OF RISK IN DHS

In previous pages, we describe ways that the existing risk efforts at DHS can successfully achieve a national risk assessment, contribute to the national preparedness system, provide greater transparency across the homeland security enterprise, and provide structured, prioritized input to S&T for their planning and budget cycle. Now, we turn the discussion to the language that the field of risk management has inherited from banking, insurance and finance, which has made understanding and collaboration in the homeland security context more difficult.

Observations: The Terminology of Risk in DHS is Problematic

Because of the efforts of DHS personnel, a common language of risk is beginning to penetrate the department. But there are two problems with the lexicon of risk as it has developed.

- Many professions and communities besides homeland security use risk language. Therefore, when DHS tries to expand risk management beyond the department it will discover that other definitions dominate other parts of the “national enterprise”—especially in the business community. The result will be confusion within the homeland security domain unless we find a new way to express the meanings intended.³⁶
- Even if terms and definitions were clear to all, the entire risk endeavor is based on the negative concept of “risk reduction.” This idea is inherently difficult to communicate to the public. Political reality demands a positive expression (“we are safer”) rather than a negative (“our risk of attack has been reduced”).

The Language of Risk

For decades before the homeland security community began to talk about risk management, the concept was described, taught, and practiced in other fields with entirely different—even antithetical—goals in mind. While most homeland security professionals think of risk as something to be avoided, professionals in banking and finance have long studied risk for the purpose of understanding how to exploit it safely in the interest of profit.³⁷

³⁶ The term “national enterprise” is itself a great example of how quickly terms become muddled when borrowed from one discipline and used in another. Who is in the “National Risk Management Enterprise?” Bankers, doctors, law enforcement, mayors and DHS officials will all have different answers.

³⁷ Frank Knight, *Risk, Uncertainty and Profit* (New York: Houghton Mifflin Company, 1921). This economics text was perhaps the first publication in the United States to suggest that profit is

As the market limitations of the Cold War gave way to explosive globalization in the 1990s, economic consultants like Peter Bernstein began to argue that “the capacity to manage risk, and with it the appetite to take risk and make forward-looking choices, are key elements of the energy that drives the economic system forward.”³⁸ In other words, without taking economic risks, there could be no economic progress.

Then in the immediate aftermath of 9/11 it appeared that the insurance industry would prove incapable of managing the economic risk posed by terrorism. Many, like David Moss, found the solution in the emergence of the government as risk manager. His concept of risk management was tied to law, bankruptcy protection, insurance, and the printing of money. This pointed to the suggestion that government intervention was required to make up for a “failing of capitalism”—that the private market for risk was frequently inadequate to promote growth.³⁹ Many others took up this “lesson” of 9/11 after devastating hurricanes along the Gulf Coast drove insurers out of the market in many places and left states as the insurers of last resort.

By early 2008, as the GAO was pressing DHS to improve the use of risk management to reduce risk, major corporations were using the position of “Chief Risk Officer” to expand their exposure while supposedly transferring it to others. Financial authors were explaining that the uninformed might think that

Risk management is a continual process of corporate risk reduction. But we mustn’t think of the modern attempt to master risk in defensive terms alone. Risk management is really about how firms actively select the type and level of risk that is appropriate for them to assume In this sense, risk management and risk taking aren’t opposites, but two sides of the same coin.⁴⁰

In other words, as DHS was establishing risk management as a way to reduce unwanted outcomes for the nation, the financial industry was using the same language in its efforts to increase risk exposure and thus increase profits. Eventually this aggressive pursuit of risk failed spectacularly, nearly destroying many major corporations, and endangering the national and global economic systems.⁴¹

By 2009, as a new administration was striving to make their interpretation of risk management a core element of homeland security, Douglas Hubbard and other financial experts were proclaiming “the failure of risk management.” Hubbard’s diagnosis was that maximizing and transferring risk was perfectly acceptable, but corporate risk managers had been doing it wrong—with inadequate data, inadequate rigor, and inadequate

the reward that an entrepreneur receives for taking an uncertain risk. Thus, risk is not to be avoided but to be embraced with care.

³⁸ Peter Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley & Sons, Inc., 1996), 3.

³⁹ David Moss, *When All Else Fails: Government as the Ultimate Risk Manager* (Cambridge, MA: Harvard University Press, 2002), 1-3.

⁴⁰ Michel Crouhy, Dan Galai, and Robert Marx, *The Essentials of Risk Management* (New York: McGraw-Hill, 2008), 1.

quantitative expertise.⁴² Other experts popularized the view that we can never conquer uncertainty, and thus the utility of calculating risk is limited. Nassim Taleb has become the “guru” of this school, arguing in *The Black Swan* that the more resolutely we pursue certainty through risk management, the more vulnerable we make ourselves to overconfidence and surprise. His solution is redundancy and resilience.⁴³

The result of this coincidence of events was that DHS began its special push to use risk management as an aspect of national preparedness just as the terms and concepts were being associated by the public with a global financial failure. Mayors, fire chiefs, and even members of DHS have since wondered about the utility of risk management to national security when the failure of the best risk experts nearly created a second Great Depression.

Risk management also has an established history—and therefore a known language—in other fields, such as medicine, engineering, and food and drug safety. These areas adopted risk management not to inform decision makers or to prioritize solutions to calculated dangers (as the homeland security community intends), but to eliminate those dangers through testing and redundancy.

In engineering, for example, risk management promotes a uniform degree of safety. Risk is not “managed” in the construction of bridges to decide which ones are most critical so resources can be allocated to make them safer, while less trafficked bridges with an increased likelihood of collapse are shorted. Such an approach to the construction of buildings, or the production of jet engines would be considered immoral and illegal. Yet deciding how to concentrate resources to reduce risk in one area, while accepting risk in another, is precisely how homeland security officials use risk tools. Thus, engineering and homeland security use the same language of risk to express quite different concepts.

In law enforcement, emergency management, and other response fields, operators see risk more like homeland security officials (as something to be reduced) rather than as engineers (as something to be eliminated). But responders see risk as something to be reduced uniformly, not prioritized, as the following attests.

⁴¹ On one hand, the authors of this citation did not encourage blind maximization of financial risk, and made it clear that solid data, careful calculation, a detailed understanding of the entire context of the risk, and a culture of informed decision making at the top were all essential for successful risk management. On the other hand, their concern was not risk, *per se*, since higher risk produced higher returns, interest rates, etc. Their concern was uncertainty, and they argued it could be conquered by systematically transferring ever higher risk to others using complex financial instruments.

⁴² Douglas Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* (New York: John Wiley & Sons, 2009). The authors proposed solution can be summarized in three words: “better quantitative analysis.” (p. xii)

⁴³ Nassim Nicholas Taleb, *The Black Swan* (New York: Random House, 2010). See especially the recommendations concerning robustness (another term for resiliency) and redundancy on pp. 370-371.

- Fire prevention and building codes reduce risk in all buildings, not in a select few because populations there are more important.⁴⁴
- Law enforcement seeks to reduce the risk of workplace violence, but not by accepting increased violence someplace else.

And even when responders do have to prioritize limited resources, as when facing a hurricane or earthquake, the driving consideration is how to reduce risk to more people, not more important people.

To sum, public safety has—as with engineering—long used some of the language of risk management, but not in the way DHS currently intends.

Finally, the experience of the Department of Defense under Secretary Donald Rumsfeld must give pause to any other government agency considering the adoption of risk management. Fresh from industry where managing risk meant trading it, not eliminating it, Rumsfeld pushed his subordinates to reduce cost and increase efficiency by taking a similar view. He personally directed the Quadrennial Defense Review in 2001 in an effort to align the department with his views on strategy and management. The result was the proclamation that “managing risk is a central element of the defense strategy,” addressed through “a new, broad approach to risk management.”⁴⁵

But managing the risk of reductions to administrative staff or timelines for weapons development turned out to be much different from managing risk against a thinking adaptive enemy. In one famous example, Rumsfeld disagreed publically with the Army Chief of Staff concerning the risk posed by limiting the ground troops deployed for the initial phase of the Iraq War. Elsewhere, he reduced forces in Afghanistan to concentrate on Iraq, accepting a long-term risk from Taliban forces in the process. He resisted a congressional effort to increase Army end-strength in order to save resources. And in many other ways, large and small, he fought the traditional military instinct to minimize risk in favor of accepting it or trading it off.⁴⁶

⁴⁴ As part of researching this paper, in early 2011 the author interviewed a fire chief in Texas.

Asked for an example of his risk management program, he said, “Twice a year we go door to door handing out smoke alarms. We hit every house.”

⁴⁵ Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, September 30, 2001), 57.

⁴⁶ This is the author’s personal analysis based on 24 years experience researching, writing and teaching national, military and homeland security strategy. As a former military speechwriter and Dean of Faculty and Academics at the National War College, I watched Mr. Rumsfeld’s language, remarks, interaction with other officials, and his release of approved official documents closely when he arrived in office. His insistence that the Department of Defense accept more risk in its plans, management and operations was a major theme of his regime before 9/11, and drives the vision outlined in the Quadrennial Defense Review dated 30 September 2001. See especially Chapter VII Managing Risks, pp. 57-65. As he repeatedly made clear, this document represented the way he expected DOD to align with his personal vision. The other examples cited represent my interpretation of how his attitude toward risk played out in

It is important to note that Rumsfeld's efforts in the Iraq and Afghanistan wars bore little resemblance to the methodical pursuit of a risk cycle and calculation of risk assessments that DHS intends today. In fact, the best indicator of his approach to risk during the wars was the famous list of possible negative outcomes that he kept in his desk drawer. He was sensitive to the downside of the risks he proposed, but his personal decision-making style was not informed by careful mathematical calculation.

But that is the whole point of this comparison. Because of the high profile Rumsfeld gave to risk management early in his tenure, subsequent problems with the prosecution of the war reflected poorly on the concepts of risk identification and manipulation. The result is a lingering skepticism about risk in some quarters, even as DHS tries to take a more measured and holistic approach.

To summarize, DHS does not own the language of risk, and using terms already well established in other contexts is likely to prove problematic as DHS expands risk management to a "whole of nation" focus.

The Communication of Risk

Those working on risk issues in DHS have done a good job of emphasizing the importance of risk communication to stakeholders and interested communities. However, the cards are stacked against successful communication, because "risk management" is a negative concept—a concept about reducing the likelihood or consequences of a bad outcome. Capturing the positive aspects of a negative action is a difficult communication challenge. In the resulting confusion, public confidence may be reduced rather than increased.

Analysts in other professions are able to successfully use the language of risk to discuss specific professional situations with other professionals in their fields. For example, doctors talk about reducing the risk of infection. Engineers discuss reducing the risk of structural failure. Financial planners speak about reducing the risk of default.

But the concept fails when it has to cross jurisdictional, organizational, disciplinary and public-private boundaries. For example, the organizations suggested by the following slogans would be unlikely to advertise in this manner:

- "Our hospital has a smaller risk of complications after surgery!"
- "Our aircraft engines have less risk of catastrophic failure!"
- "You are less likely to lose your money with our bank!"

In communications to the public and across specialties, leaders and operators in fields like medicine, banking, and engineering instead emphasize the *positive* vision of what they want to achieve—as the following examples show:

national security affairs during the rest of his term in office. This is my personal analysis, and does not reflect the opinion of any other person or organization connected to this white paper.

- Improved deterrence.
- Improved defense.
- Improved safety and security.

In the myriad of media retrospectives on 9/11 over the last decade, no one has asked, “Has the risk been reduced since then?” Instead, interviewers consistently ask, “Are we safer today than we were then?”

The concepts of risk management and risk-informed leadership are often contrary to public leadership, and drag leaders into a discussion of what they want to *prevent* instead of a vision of what they want to *achieve*. This is not beneficial to DHS or the rest of the federal government.

This is not to suggest that the effort currently identified as risk management has been wasted or should be abandoned. In fact, the progress DHS had made in risk management since 2001 (particularly in the last two years) has been noteworthy. The organizations, definitions, tools, coordination, and products of the department are maturing to the point that they can provide valuable guidance to decision makers if used and presented in a useful way. But to succeed, homeland security risk management needs its own language, which those within the homeland security enterprise can create and control. And that language needs to express the goals of risk management in positive terms—what is to be increased—not the negative terms of what is to be reduced.

Recommendations: Rethinking the Language and Communication of Risk in DHS

The linguistic challenge of using risk in conjunction with homeland security is difficult and complex. The solution is short and simple.

Change the Concept and Language

Replace *risk* and its associated terms with a concept and body of terms and processes that DHS owns and can focus on the homeland security mission. The idea here is to save the risk-related work already accomplished by creating a substitute concept, language, and logic that DHS controls, that the average responder, manager, and senior leader can understand, and that applies to homeland security alone. Here are several examples:

- *Safety and security* rather than *risk*.
- *Improving safety and security*, rather than *reducing risk*.
- *Safety and security assessment* rather than *risk assessment*.
- *Safety and security improvement analysis* rather than *risk analysis*.
- *Integrated safety and security management* rather than *integrated risk management*.

Communicate Risk Reduction in a Positive Way

Change the focus from reducing the problem to improving the solution. Other examples, like the ones given above, include the following:

- The DHS grant program becomes “Federal Assistance for Improving Safety and Security;”
- The measure of DHS Science and Technology projects becomes how well they improve safety and security;
- Metrics at every level would measure progress at improving safety and security, not just reducing risk;
- Decisions would be informed by how to best improve safety and security, not reduce risk;
- The department’s mission and operations—which frequently seem bifurcated between prevention/protection and response/recovery—would be unified since all these measure improved safety and security, and
- The national risk assessment and the National Preparedness Plan would focus on improved safety and security.

This solution still requires a risk assessment; the department needs to prioritize between dangers. DHS would still need to know

- what can happen,
- how likely it is to happen, and
- what is the severity of the consequences .

However, the questions that those in DHS *risk management* currently answer would be even more appropriate if the department addressed them in the context of *safety and security management*—as the following questions illustrate:

- What can be done?
- What options are available, and what are the costs and benefits of each?
- What impacts do current decisions have on future options?

The new language might also result in the following different priorities and decisions:

- Under safety and security management, DHS might focus time, money and attention not on the biggest problem, but on the most promising solution (i.e., the biggest improvement in safety and security).
- A focus on achieving safety and security (vice reducing risk) would likely serve to bring the DHS and intelligence communities closer together. As a significant report on the subject pointed out, the dysfunctional relationship between the two communities seems to be rooted in the unfamiliar and sometimes counterintuitive language of risk.⁴⁷

In short, the language of risk is unfamiliar to many in DHS—and complex and confusing to the rest, because the meaning of the language is different from what they expect. Success in risk management is challenging to communicate, as it must convey a double negative (the reduction of a bad thing) as a positive outcome.

On the other hand, a small but profound change to a few key terms (substituting *safety and security* for *risk* in risk management) could improve the utility of the risk program dramatically.

⁴⁷ John Baker et al., *Risk Analysis and Intelligence Communities Collaborative Framework* (Washington, DC: Homeland Security Institute, April 23, 2009), 45.

PRACTICING RISK THINKING

Given the time and effort required to implement risk thinking and practices into planning and operations across the entire nation, an obvious question is, “Why do it?” Why has DHS decided to “incorporate the risk management process into the overall mission and management of the department?”⁴⁸

After all, risk management is a relatively new concept as applied to national security issues, and does not boast an impressive history of accomplishment in the private sector over the past decade. Why push the concept of integrated risk management to share risk information and process across the entire homeland security enterprise nationwide?⁴⁹

Observations: On Risk-Informed Decision Making

The answer is that the Department of Homeland Security has no choice but to prioritize risks. As observed in the earlier discussion on the National Risk Assessment, achieving the vision of a nation that is “safe, secure and resilient against terrorism and other hazards” would itself threaten both our economy and our liberties if DHS tried to prevent everything bad from happening everywhere, all the time.⁵⁰

But when decision makers turn to analysts for help in prioritizing scarce resources, they are frequently looking for simpler ways to visualize and understand the threats they face and the responses they might mount. Depending on what information those leaders receive and how it is provided, the process of *risk management* might create new risks -- by misleading the people it is supposed to inform.

For example, narrowly applied, risk management can suggest a false simplicity or overconfidence in the analysts’ calculations. Risk management might also suggest too great a role for federal organizations, or discourage other jurisdictions from participating. It might bias solutions in a particular direction, or minimize the complexity of the challenges faced. Wrong or narrow management processes may actually increase danger rather than reducing it.

Some Warnings from the Past

As history demonstrates, the consequences of evaluating risk but getting it wrong can be severe.

⁴⁸ Directive 007-03, 6.

⁴⁹ *Risk management* is the process by which an organization identifies and deals with risk, while *integrated* risk management is the active sharing of risk management information and actions across the larger enterprise of which that organization is a part. The *DHS Risk Lexicon* defines the terms more completely (pages 30 and 19 respectively). See Appendix A to this paper.

⁵⁰ *Quadrennial Homeland Security Review Report*, vii.

- The risk that Charles V of Spain accepted when he concentrated his fleet for the invasion of England helped precipitate the defeat of the Spanish Armada. Spain never recovered its position as world leader.
- Technical experts advised that Pearl Harbor was too shallow for Japanese naval torpedoes, the Philippines too distant for attack by Japanese ground-based aircraft, and the danger from sabotage greater than that from air attack. This thought process led American commanders to accept risk that cost them dearly on December 7, 1941.
- President Truman thought there was little risk that the North Koreans would engage the U.S. military when he sent a small force to oppose their advance in 1950. General MacArthur dismissed the risk of Chinese entry into the war in 1951.
- President Eisenhower thought that the risk of losing a spy plane was small when he denied that U2 flights were taking place over Russia.
- President Kennedy underestimated the risk of nuclear war in the Cuban Missile Crisis.
- President Johnson thought he had accounted for the risk of sending more troops to Vietnam.
- President Carter was told there was little risk to admitting the Shah of Iran to the United States for medical treatment.
- President Reagan's military advisers underestimated the risk to Marines sent to Lebanon.
- And in the aftermath of Vietnam, both Congress and several American administrations saw the risk of abuse to civil liberties to be greater than the risk of terrorist attack, and so erected a "wall" between domestic intelligence and law enforcement – a wall that came back to haunt us in the 9/11 disaster.⁵¹

In short, properly conducting risk assessments is not enough. DHS must effectively and accurately convey both the risks and the limits of the department's knowledge to decision makers. Risk management and integrated risk management should produce fully informed decisions, not just simplify the decision-making process.

⁵¹ There are many examples of *successful* risk management, such as Eisenhower transferring risk away from the D-Day beaches, or Roosevelt accepting risk in the Pacific to concentrate war winning forces in Europe. Further examples include President Kennedy accepting technical and political risk in waging a public "race to the moon." But successful risk management tends to be overlooked or forgotten, while failures at risk management become historical object lessons. And for DHS, the failure of risk management endangers the nation.

Better Understanding through Risk Typology

One way that risk analysts and risk managers might lead decision makers astray is by misleading them about the nature of risk itself. What is represented as a simple linear calculation of risk may obscure much more complex cause and effect relationships. Retired Coast Guard Captain Bob Ross (now a DHS employee) has created a useful typology to describe these varying levels of complexity, the varying types of risk, as well as the reason that some mathematical tools might work well for one type of risk—and not at all for another.⁵²

As he explains it, risk may be grouped into:

1. Stable and easy to discern.
2. Stable but difficult to discern.
3. Dynamic Natural.
4. Dynamic Adversarial.

Stable Risks

A stable risk is one in which neither the hazard nor the systemic context in which the hazard resides change in direct response to risk management actions. A simple safety issue like rising water is one example; other examples include common issues that structural and electrical codes address. Solutions may be as simple as “fight or flight” or, for more technological risks, measures such as creating engineering standards, licensing key personnel, and establishing sound operating procedures.

Type I Risk (Stable and Easy to Discern)

This type consists of those risks whose existence, nature, likelihood, and consequences are obvious—marked by an easy-to-discern pattern of cause and effect. Little is required in the way of mathematical analyses to assess Type I risks, but engineering or other sophisticated analyses aimed at determining causal factors and remedies may well be required.

Type II Risk (Stable but Difficult to Discern)

This type differs from Type I in that these require extensive analyses to determine their nature, likelihood, consequences, and maybe even their existence. Examples include cancers potentially caused by workplace exposure to suspected carcinogens, and risks arising out of large but bounded engineered systems, such as commercial aircraft or nuclear power plants. In the latter, rigorous analyses are required to identify and address potential failure points and modes. Disaggregation of the problems and the integration of several solutions may be necessary. But at the end of this process, the system remains essentially what it was originally, and potential causal factors—such as a failure-prone pump removed from the design—are not reintegrated back into the system.

⁵² Bob Ross, *Risk Analysis, Risk Management, and Risk Type: An Historical Perspective*, unpublished manuscript, revised 2011. The author thanks CAPT Ross for taking a personal hand in crafting the text describing his typology in order to get the description right.

Dynamic Risks

This risk exists when either the hazard or the systemic context in which it resides, or possibly both, can change as a direct result of risk management actions. A further complicating factor of dynamic risks is that they are typically found in unbounded, complex adaptive systems whose behaviors and properties may not be discernable through analyses or predictable. Examples include unanticipated driver reactions to new traffic control measures and drug smuggling patterns that shift in response to changed law enforcement measures.

Type III Risk (Dynamic Natural Risks)

Type III risk arises in natural systems where the components are acting according to physical or biological laws (e.g., ecosystems). These risks also arise in human systems where human error—rather than purposeful intent—plays a role. Vessel traffic in a modern seaport and the potential for antibiotics to make bacteria drug-resistant are good examples of mixed natural and human Type III risk. In both cases, seemingly beneficial risk interventions may be ineffective (e.g., aimed at the wrong causal factor) or may trigger unintended systemic adaptations that leave the recipients worse off than before.

Type IV Risk (Dynamic Adversarial Risks)

This type of risk involves what has been known as “game against Adversary” or a “thinking enemy.” The opponent may not be an “enemy” in the traditional sense of the word, but the opponent can seek to overcome efforts to defend against or mitigate the effects of his actions. Examples of dynamic adversarial risk management include efforts as simple as an adult trying to reduce the risk of accident in a home with active and inquisitive toddlers, and as complicated as counterterrorism.

Dynamic Risks in the Context of Homeland Security

Types III and IV are closely associated with what are commonly called “wicked problems”—*wicked* meaning fiendishly difficult to address due to political and social factors on top of already staggering system-of-system complexities.⁵³ Thus, the more complex the problem, the greater our uncertainty, and at the same time, the greater the likelihood of cascading effects. That seems to hallmark the field of homeland security, where the more complex risks are generally the more dangerous. Exploring these two risk types further, then, is pertinent for DHS, to inform the department’s risk thinking.

For example, the Japanese earthquake that became a tsunami that spawned a radiation disaster represents a “wicked” Type III risk. That is, two Type I/II risks (earthquake and tsunami), mixed with human failures and Japan’s earlier decisions to address their energy-dependence concerns with nuclear power, and grew into a Type III risk.

⁵³ Horst Rittle and Melvin Weber, “Dilemmas in a General Theory of Planning,” *Policy Sciences*, 4 (1973), 155-169. Many articles address the issue of “wicked problems” today. This article was one of the first.

A major cyber attack that causes cascading critical infrastructure failures would be another “wicked” Type IV risk. Such a risk would occur with systems built to address previously identified Types I, II, and III risks.

A major point that Ross makes by establishing this typology is that Type III and IV risks are the most common facing homeland security, and the nation is the least prepared to recognize and address them. As he explains,

The fields of risk analysis and risk management have developed considerable bodies of knowledge and practice. Moreover, they have had some significant successes. But careful examination of those successes will reveal many of them to be Type 1 and 2 risks. More noteworthy is that recent large risk management failures – 9/11, the Deepwater Horizon oil spill and the financial market near-collapse – were all due to Type 3 or 4 risks. As scientific, decision-support and...Recognizing that Type 3 and Type 4 risks exist, and that they are qualitatively different in very significant ways from Type 1 and 2 risks, is a necessary first step in coming to grips with them.⁵⁴

Homeland security risks are complex mixtures of these various types. Simple computational solutions to simple types of risk (I and II) are, at best, ineffective—and misleading at worst, in the more complex situations (Types III and IV).

Additional Causes of Misperception

An additional problem that Type IV risks pose is that human opponents are not just interactive; a “thinking enemy” learns, so the threat is constantly changing. Earthquakes, tornadoes, and hurricanes do not become smarter over time. However, defensive efforts can drive an enemy to a corresponding change in offense. He learns from the experience and become more sophisticated, which increases the risk to the defender. Thus, the act of risk management—essential as it is—can drive an enemy to creative efforts that may *increase* risk and uncertainty. Recent examples by opponents of the United States include putting a bomb in a printer to disguise its electronics from detectors, and putting a bomb inside a dog to be shipped on an aircraft. The result is a dangerous irony: the better we are at risk assessment and risk management, the more we may be led to overconfidence when an enemy takes an unanticipated leap.

Another aspect of risk management that can lead decision makers astray is the very bureaucracy charged with carrying it out. Bureaucracies standardize procedures. They replicate success. When an organization thinks it is successful, instituting a major change in thinking (like the adoption of new risk management terminology and practices) is difficult. Such an organization must see its own shortcomings or a clear promise of improvement before it will accept internal change brought on by an external influence.

⁵⁴ Ross, personal comment / update to his unpublished manuscript. In order to pursue these ideas further, I recommend that future researchers contact CAPT Ross personally to investigate how his thinking has evolved.

The report of the 9/11 Commission offers a warning here, with an entire chapter devoted to the point that before the September 2011 attack “The System Was Blinking Red.”⁵⁵ Individuals recognized that there was a problem, but the bureaucracy actually prevented recognition of the new risk and doing something about it. The failure, the commission concluded, was not one of information but of *imagination, policy, capabilities and management*.⁵⁶

In other cases, the “system” is not blinking at all, because data to inform risk calculations is hard to come by—or is ignored. In such a case, the use of quantitative methods to present inherently uncertain results may lead to false confidence.⁵⁷ Or the presence of a system may lead a leader to conclude that analysis is being conducted when it is not.⁵⁸

Another way that risk management can cause the customers it serves to miss the mark, is through simple cultural or professional misunderstandings. One of the striking observations of a 2009 study of the interaction between risk analysts and the intelligence community was how frequently their expectations on threat information “pass in the night.”⁵⁹ Uncertainty is more common in threat analyses than is certainty. Information on vulnerabilities is generally local in nature, and jealously guarded—especially by the private firms that own most public infrastructure. The system-wide consequences of point failures (especially of CI/KR) remain a frequent feature of the evening news. Such realities are frequently well understood by one side of the risk-intelligence partnership, but a complete surprise to the other.

Also, the way in which policy is written, risk is calculated, and management is cycled. This can be a barrier to an organization’s adoption of risk management—or to changes in such management.

⁵⁵ *9/11 Commission*, 254-277.

⁵⁶ *Ibid*, 339.

⁵⁷ “The Black Swan effect” is a term used to describe events which are so removed from historical reality—impossible to anticipate—that they simply are not imagined. This author is equally concerned about what he calls “The Red Motorcycle effect.” Because motorists do not expect to see a motorcycle in traffic, they sometimes look directly at one and just do not comprehend what they are seeing. The same may be true of events. So we may be led to false confidence either because we cannot anticipate an event, or because the system we have built refuses to do so.

⁵⁸ Apparently this is what led Secretary of Homeland Security Napolitano to observe “the system worked” in the immediate aftermath of the attack by the “Underwear Bomber” (December 2009) – when in fact the system in place failed to collect and process ample evidence of the attacker’s intent.

⁵⁹ Baker, 45. “In particular,” Baker writes, “risk analysts sometimes have unrealistic expectations concerning the ability and willingness of intelligence analysts to produce quantifiable threat inputs. . . . Likewise, intelligence analysts typically expect risk assessments to account for uncertainty at levels of detail that can create unmanageable complexity for risk analysts.”

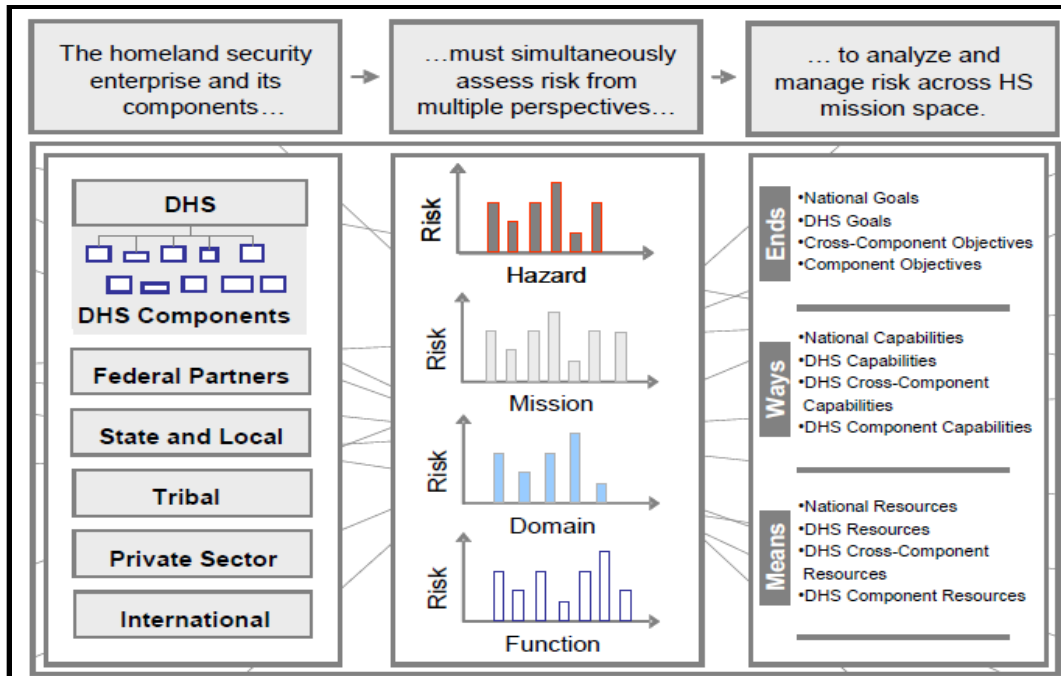


Figure 1. A Conceptual View of Integrated Risk Management⁶⁰

Within DHS, one example of a barrier to fully appreciating the risk management information available may be found in the “Framework for Risk Management,” a touchstone concept for understanding risk as DHS views it.⁶¹

As the proposed foundation for follow-on policy, doctrine, and guidance, the framework simply outlines a vision, objectives, principles, and process for integrated risk management. It is an internal DHS document, intended primarily for an internal DHS audience. The view of homeland security which it reflects (as shown in Figure 1 above) is therefore decidedly “DHS-centric.” Although state, local, tribal, and private sector partners are mentioned, there is no discussion of their role. There is no place reserved for their input—no consideration of their risk, goals, functions or resources—no provision for DHS to respond to their needs or opinions. The effect is to suggest to readers within and without the department that homeland security risk management begins and ends with federal direction, with other participants playing the role they are assigned.

⁶⁰ *Framework for Risk Management* (Jan 2009), 3.

⁶¹ *Ibid.* 3.

A second example of how a well defined system may suggest an inclusiveness of information which does not exist (and thus mislead a decision maker) is offered by the DHS risk management process, which consists of six phases conducted in sequence, with risk communication an important aspect of every phase.



Figure 2. DHS Risk Management Process⁶²

The document is clear that this process is intended to support the department, and is compatible with the work of other approaches like the National Infrastructure Protection Plan, the GAO, the DHS Target Capabilities List⁶³, and even the International Standards Organization (ISO) 31000 standard. Again what it leaves out is any suggestion of the use of, or integration with other jurisdictions in the homeland security enterprise.

Nothing about this approach suggests that DHS decision makers should consider state, local, tribal, or business concerns, or approach decision makers from those jurisdictions to coordinate their efforts. The major problem here is not that the DHS process is intentionally exclusive. It is that it missed an excellent opportunity to make risk thinking broadly inclusive.

Also, the way risk is calculated may sometimes drive decision makers to consider the type of threat more than the consequence of the event. Consider a nuclear weapon

⁶² Ibid, 8.

⁶³ Department of Homeland Security, *National Incident Management System* (December 2008), 11. The Target Capabilities List (TCL) identifies a national network of capabilities needed for national preparedness for natural or man-made disasters.

detonated in the desert versus a lone gunman at the Super Bowl. Considered from the perspective of threat x vulnerability x consequence, the focus would be drawn to the threat of the nuclear weapon, no matter the numerical calculation of risk. Now consider the change in perspective if the order of consideration were consequence x vulnerability x threat. This time, even if the numerical calculations were exactly the same, the significant consequences of many dead at the Super Bowl might outweigh the consequences of an explosion in the empty desert. The whole focus of risk management would shift.

Finally, in thinking about how risk may inform decision makers, consider the interaction, as follows, between elements of risk—not just their overall product:

- Changing the *threat* (by reducing the availability of precursor chemicals) might reduce *vulnerability* (by forcing the use of less effective chemical compounds) and thereby lower the *consequences* (less power against a target) of a chemical attack.
- Changing the *consequences* (by improving biological response) might reduce *vulnerability* (fewer people apt to become sick), which might deter the investment of time and money in creating a biological *threat*.

The point is that reducing risk to a quantitative value—like the number of precursor chemicals, in the example above—can suggest a static condition requiring an isolated, static decision. Furthermore, prioritizing a list of calculated risk values may seem as simple as approving their numerical ranking. But risk—especially from a thinking enemy—is dynamic, constantly changing. The act of allocating resources against risk may change vulnerability, consequences, and hence threat (or intent). Risk management does not just reduce risk, it can produce unintended impacts in other areas, as well. Decision makers in DHS should be made aware of this dynamic interaction of factors, and the full range of the changes their actions are likely to cause.

To summarize, depending on what information is provided and how, *risk management* risks misleading the decision makers it is supposed to inform. It can, of course, be a great assistance in identifying relationships between threat or hazard, vulnerability, and consequence. Risk management can also suggest the best ways to prioritize solutions. But there are other, negative things it might also suggest to DHS decision makers—for one, a false simplicity or overconfidence in the department's calculations. Risk management might also suggest too great a role for federal organizations, or discourage other jurisdictions from participating. It might focus attention in the wrong direction just by the way it is presented. Or in an effort to make risk manageable, DHS risk analysts and managers may so reduce the questions and simplify the answers that the complexity and interactive nature of the problem is obscured. Improperly applied, the department's own risk management system could mislead decision makers, producing increased danger instead of improved safety and security.

Recommendations: Explaining Better the Risk of Risk

Given the ways in which risk managers might inadvertently mislead decision makers in attempting to present complex ideas, what can DHS do to help everyone in the risk management cycle of the department better understand and visualize the risk they are seeking to manage? Here are two distinct suggestions for explaining risk better. The first describes new ways to *visualize* risk information. The second offers new ways to *conceptualize* risk operations.

Visualize Risk Information

The single best answer for conceptualizing risk operations may be for the risk manager in DHS to remember his or her proper role, which is “not to try to read a crystal ball, but to uncover the sources of risk and make them visible to key decision makers and stakeholders in terms of probability.”⁶⁴

This means that, just as risk managers aggregate information and simplify calculations to aid decision makers, they must be ready to disaggregate the information and display it clearly for comparison. A survey of other approaches to risk management outside the field of homeland security offers a wide array of other tools for visualization and understanding, including the following:

Risk Display Table

This is a simple list of the following five columns:

1. Target,
2. Threat,
3. Vulnerability,
4. Consequence, and
5. Risk (T x V x C).

The table is not a model. It does not show or otherwise account for calculations, weighting, or other factors. It is simply a display of risk factors and calculated risk values from a model. If desired, it could be reduced to two columns, target and risk. The table serves to give decision makers a broad view of all the risks they face in a particular jurisdiction.

Threat Registry Table

This may be used for all applicable threats and hazards (chemical, biological, radiological, nuclear, explosive, natural disaster, maximum of maximums, etc.). Threats are listed without ranking—for completeness and consideration.

⁶⁴ Hubbard, 18.

Target List

This list may be a simple roll of important assets that an enemy might hit, listed in no particular order or group, or perhaps grouped in ways that provide specific emphasis beyond the pure calculation of risk. Groupings might include the following:

- Potential deaths/injuries;
- Population directly impacted;
- Geographic region (downtown, rural, etc.);
- Type of impact (economic, tax base, population density, etc.), and
- Ownership (private, commercial, government, federal, etc.).

The goal is to show decision makers the relationships that are not immediately visible when one compares only computed risk. For example, when a significant number of at-risk locations belong to a single responsible party (like a school system or a private industry), decision makers might realize major advantages from focused investments.⁶⁵

Target Map

This map consists of the same information as a target list but is overlaid on an electronic geographic information system. Visualizing either the concentration or separation of targets could change the decision maker's evaluation of relative risk. Once displayed in relation to all of the targets, other important factors (road grids, electrical grid, flood plains, etc.) may attract consideration.

Threat Probability Table

This is a list of threats by target and type of event (chemical, biological, radiological, nuclear, explosive, natural disaster, cyber, etc.). Threats are grouped by the likelihood of occurrence and are color-coded by type. The goal is to help decision makers recognize special risks that might have low-risk value but high-risk value in some other way—for example, a low likelihood terrorist threat against a small, inconsequential target may nevertheless have high-risk from loss of domestic confidence in government.

Threat Probability Map

This contains the same information as the threat probability table, but shows geographic relationships. Any concentration of threats or hazards deserves special attention. An example of this is when a number of chemical risks in close proximity might call for resourcing special equipment, even though the risk calculations of individual targets alone indicated that the priority was too low for such expenditures.

⁶⁵ Some of the proposed “tools” listed here represent applications to the field of homeland security of constructs used elsewhere in thinking about risk. However, most of the ideas in this section are ideas generated by the author.

Threat Response Display

This display is applicable for all identified threats (all chemical, all high-threat chemical, all federal chemical, etc.) and shows what jurisdictions have the resources required to respond to them. Individual agencies could use this display with the National Infrastructure Protection Plan to evaluate needs, capabilities, agreements, etc. And it might impact grant allocation, as jurisdictions are encouraged to pursue support agreements in lieu of buying individual capabilities. The display could be color-coded for emphasis.

Threat Response Map

This map contains the same information as the threat response display but shows geographic relationships, agreements, etc., between responders and jurisdictions. Again, seeing the geographic dispersal provides a special perspective on problems and solutions that are not visible when considering just risk calculations.

Risk Matrix

This is a simple four-cell matrix with vulnerability x consequence on the “x” axis, and threat on the “y” axis. Specific targets are then arrayed in the cells according to their individual characteristics. The cells could be color coded with red for the upper right “High/High” quadrant, and green for the lower left “Low/Low” quadrant. A risk matrix can be used to display many otherwise-hidden aspects of risk analysis. For example, the target groups in the High-High or Low-Low quarters might share some characteristics that modify the way risks are addressed or funding is allocated. An example of this is when a high proportion of risks from a flood suggest a unified effort at flood mitigation, rather than individual protection projects for multiple locations.

Vulnerability Reduction Display

This display may be used for selected targets (locations, types, etc.) grouped by the change in vulnerability when resources are applied. The display could be modified according to what resources are already available for sharing, thus showing what whole-of-community actions would be effective even without new funding.

Consequence Reduction Display

This display would be similar to a vulnerability reduction display, except it would show the impact of specific actions on reducing contagion and cascading effects in the aftermath of an event.

Impact Table

This table might show the variety of impacts (financial, health, legal, transportation, by type of CI/KR, etc.) from different types of attacks on different targets. The purpose is to help decision makers get beyond the simple calculation of risk to see how different risks impact different aspects of the homeland security enterprise.

Cascade Matrix

By putting individual targets and types of attack on one axis, and the entire range of CI/KR on the other, it is possible to rapidly display how events of one type in one place might cascade throughout the homeland security enterprise. For example, a successful attack on the electrical grid would cascade immediately through most other elements of critical infrastructure. On the other hand, an attack on agriculture would have little impact on dams or transportation.

Severity Table

Severity is defined as the calculated risk of an event (generally specified in dollars) plus the cost of response. Such a display will serve to separate out for consideration low risk-high consequence events from high risk-low consequence events, where traditional risk analysis might calculate similar scores and thus obscure the difference mathematically.

Correlation Expectation Table

This visual display of data would allow decision makers to see how their proposed actions and priorities would influence consequence, vulnerability, threat, as well as risk overall. This would be especially helpful in visualizing the dynamic nature of risk, and how changing one aspect of the calculation ripples through the equation.

Risk Reduction Table

This display would be similar to a correlation expectation table, except that it would show only the changes in *risk*, not the anticipated interaction of threat, vulnerability, and consequence as well.

Presenting all of the information contained in all of these tools might overwhelm an individual decision maker. Even routinely creating all of these tools might be challenging for any organization. But working through the process of developing and populating these displays, understanding their interaction, and presenting them selectively would prepare the risk management staff of DHS to serve decision makers and the national preparedness system well. Instead of presenting flat percentages, the risk manager could inform the decision maker with rich information and a deep understanding of the calculated likelihood, impact, and uncertainties of every target.

Conceptualize Risk Operations

The above review of risk information and how it may be presented to decision makers also suggests two new concepts that should be added to risk management.

The first concept is *risk severity*. The term “severity” helps to differentiate between risks by adding the cost of success to the cost of failure (severity = risk + cost of response). If two scenarios have virtually the same risk, but one is far more costly to address, then this “severity” should be brought to the decision maker’s attention. The present simplified approach to risk calculation obscures this difference.

The second concept, the *management of risk*, is an important concept which is similar to but different from *risk management*. Risk management has been carefully defined in the DHS Lexicon as “the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost.”⁶⁶ This essentially means overseeing the risk management cycle at an appropriate level. While DHS risk literature makes it clear in several places that events can begin at any point in the cycle, the context in and consistent thread throughout risk publications suggests that DHS risk management is designed to promote *cyclical budget decisions*. That is, the cycle starts with reviewing the context and identifying potential risk, proceeds through analyzing risk and developing answers, raises these answers for decision, then implements, evaluates, and monitors the process until the cycle starts again. The decision most consistently required is the allocation of resources.

Cyclical operational issues lend credence to the idea that the risk management cycle is largely about allocating resources. The activities of the National Infrastructure Protection Plan are moved primarily by cyclical funding. The FEMA grant programs that lean heavily on risk analysis and management are connected to cyclical funding. The evaluation of current programs and identification of new risks both coincide largely with the funding cycle. Indeed, H.R. 4842 and its provisions for developing a National Threat Assessment was a product of cyclical DHS funding.

Certainly an unexpected event can initiate the risk management process at any time—as the threat of attack from a person with a bomb in his underwear resulted in new threat identification, risk analysis, alternative development, plan implementation, etc., without reference to the annual funding cycle. But on a day-to-day basis, applying the risk management cycle in DHS is generally connected in some way to the funding cycle.

But DHS managers also face changes to risk on a daily basis—new threats, new friendly capabilities, new budgetary considerations, and new issues raised by partners. And they face crises that require immediate action. DHS managers also face new challenges to the combination of threat/hazard, vulnerability, and consequence every day. There is no time in such situations to sort through the entire risk cycle—leaders have to sense the situation; collaborate with others; develop a plan of action; calculate the risk, cost, and benefit; modify and coordinate the plan; put it into action; evaluate its utility; and adjust on an ongoing basis.

These are active managerial duties that include leading, taking action, taking responsibility, and making something happen as a manager of people and resources. An understanding of risk should inform these duties of DHS risk managers. But they are far removed from the more formal process of risk management.

⁶⁶ DHS Risk Lexicon, 30.

Consider the difference between the deliberate planning involved in setting annual TSA personnel levels, and the crisis action planning required to deal with a bomb threat at a specific airport. Both require managers to deal with risk. The first falls under the classic definition of integrated risk management. The second type of planning—which is more local, more immediate, more focused on the allocation of existing resources than the procurement of new resources—needs a different term to set it apart. “Management of Risk” seems appropriate. Establishing a distinction between risk management and managing risk would be a useful course of action for DHS and its Office of Risk Management and Analysis to pursue.⁶⁷

⁶⁷ Some might argue that actively managing the results of the risk management framework (or cycle) is a subset of the framework itself— so that risk management and the management of risk are the same thing. But after years of struggling with a similar challenge, the Department of Defense has chosen to distinguish between *deliberate* action planning (similar to the risk analysis cycle) and *crisis* action planning (which includes many of the same actions, but performed along a compressed timeline). This is the same sort of distinction the author is striving to make by differentiating between *risk management* and the *management of risk*. Risk Management as DHS treats it is what the bureaucracy does on a systemic basis. It is frequently connected to the budget cycle. Managing Risk is what a port security officer does in the morning when 3 guards call in sick or he gets a security warning from the FBI. He has to move around his assets, get new assets, borrow, innovate, etc. Actions taken to address risk on this compressed timeline may include some or all of the parts of the risk management framework. But there are differences in the leadership and management skills involved in these two situations. This paper suggests that these differences are significant and should be regarded differently.

ADVANCING RISK MANAGEMENT IN DHS

Risk management has been making significant strides within the Department of Homeland Security.

Earlier in this study we used an assortment of government documents to demonstrate the growth of risk as an organizing idea for homeland security. A host of other products, programs, committees, and briefings that suggest progress in the field of risk management for homeland security were not addressed. In particular, the work of the DHS Office of Risk Management and Analysis should be highlighted. The following are just a few of their accomplishments:

- Completing the Risk Assessment Process for Informed Decision-making (RAPID)—a model for strategic-level analysis of threats, risks, gaps and budget requirements.
- Completing the DHS risk management framework, to include articulating a vision, objectives, principles, and process for integrated risk management in DHS.
- Creating a risk steering committee for the department, organized in three tiers (components, deputies, senior working staff), to govern risk management issues.
- Producing analytical guidelines for risk practitioners, providing practices and lessons learned to support education and training.
- Overseeing the publication of the *Risk Lexicon*.
- Continuing its contribution toward fielding a Risk Knowledge Center.

DHS has accomplished all of this with a dedicated staff of only 25 and a budget of about \$10 million.⁶⁸

Observations: On the Progress of Risk Efforts in DHS

What still seems to be missing is a unified vision and buy-in of a single unified approach from senior leaders in DHS.

At the same time, many other organizations in the department have also developed risk efforts, from the Directorate of Science and Technology to TSA. FEMA has produced an excellent online training program to explain risk management to people at every level across the enterprise.⁶⁹ Senior-level government policy documents, to include the

⁶⁸*Hearing before the United States House of Representatives Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, 111th Cong. (June 10, 2009) (statement of Philip Reiting, Deputy Undersecretary).*

⁶⁹<http://www.learnaboutrisk.org> accessed March 15, 2011.

previously cited PPD-8, now emphasize the central role risk is to play in future DHS activities.

Perhaps most notably, funding for the DHS fiscal year 2011 Preparedness Grant program initiative—with awards totaling \$2.1 billion—was apparently driven to a large degree by the department’s risk management process. According to Secretary Janet Napolitano, “In today’s tight fiscal environment, we are maximizing limited grant dollars by setting clear priorities and focusing on the areas that face the greatest risk.”⁷⁰ As the May 2011 press release further explains, this is in accordance with a 9/11 Commission recommendation that homeland security funds be allocated “based strictly on an assessment of risks and vulnerabilities,” to focus limited funding in the highest risk areas.”

Yet even with all of this progress the establishment of risk management within DHS has been a struggle. The full development of the concept is still far from complete, as the following evidence attests:

- Despite Secretary Chertoff’s announced intentions, risk management did not play a significant role in reshaping the structure and functioning of the department during his tenure. In fact, it is hard to find evidence that it played much of a role at all.⁷¹
- Outside evaluations by the GAO (2005, 2008), the Congressional Research Service (2007), the IBM Center for the Business of Government (2009), and the National Research Council (2010) all concluded that DHS is working on the promise of risk management, but remains far from achieving its goals.⁷²

⁷⁰ Office of the Press Secretary, “DHS Announces Grant Guidance for Fiscal Year (FY) 2011 Preparedness Grants,” May 19, 2011, http://www.dhs.gov/ynews/releases/pr_1305812474325.shtm.

⁷¹ This is not a casual comment or criticism. The author has been involved in full time researching and teaching homeland security since before 9/11. During the Chertoff tenure at DHS, the author attended dozens of major conferences, focused on what concepts should be taught in the field of homeland security. Sponsors included DHS, NORTHCOM, the Naval Postgraduate School, the National Defense University, the Army War College, the FEMA Higher Education Program, and the Homeland Security and Defense Education Consortium Association. Risk Management was never mentioned at a single conference. In addition, during this time the author hosted a national radio program that interviewed approximately 900 guests from the field of homeland security to include the Secretary of Homeland Security and his Deputy. Not a single guest ever mentioned risk management. Risk management played a prominent role in Secretary Chertoff’s relook at DHS upon his arrival in the spring and summer of 2005, and he intended to use it as an agent of change. But the focus on risk management dissipated after Hurricane Katrina, and never recovered its momentum.

⁷² GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, 2005; _____, *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, 2008; Todd Masse, *The Department of Homeland Security’s Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, 2007; David Schanzer and Joe Eyerma, *Strategic Risk Management in Government: A Look at Homeland Security* (IBM Center for the Business of Government: 2009), <http://www.businessofgovernment.org>; John Ahearne, *Review of the*

Representative of the assessments referred to above, a National Research Council report was quite blunt in its observation that

the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested. Moreover, it is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analysis other than for natural disasters.⁷³

Perhaps most surprising, as of this publication date, no speeches by the current Secretary mentioning risk management are posted on the department's web site. If risk is to be one of the animating concepts in the department, one might expect the Secretary to be making a greater point of its relevance in public.

Recommendations: Advancing the Risk Endeavor in DHS

The various risk management efforts within DHS will not become welded into a single integrated, focused and functioning program without emphasis from the top – and that means all of senior management, not just the Secretary by herself.

Building a risk management culture – so that DHS personnel think of risk management as the way they do business on a daily basis – should be a top priority. This is a complex leadership challenge treated separately in the next chapter.

The recommendations below are intended to establish the human capital – people, training and education – required if risk management is to gain both legitimacy and traction as a routine staff function in DHS. Similar actions are required by any other organization seeking to implement risk management as an integral part of their staff routine.

1. **If risk analysis is to help determine the direction of DHS, then it needs to provide positions for a professional staff to advance and support that effort.** Assigning people to work on risk as collateral duty and training them on the job sends a message that senior leaders are not serious about the subject. Furthermore, the various departments and agencies will not take risk seriously until they see serious career opportunities develop in this field. When the senior leadership of the department thinks enough of those trained in risk to invest money and other resources into expanding their presence on the staff, the departmental rank and file will begin to accept that risk thinking is here to stay.
2. **Applying risk seriously—as the Air Force has done, for example—requires a staff formally educated in the mathematical intricacies of Bayesian probability sciences.** If the accomplishment of DHS missions depends on risk

Department of Homeland Security's Approach to Risk Analysis (Washington, DC: National Academies Press, 2010).

⁷³ Ahearne, 80.

management, and risk management depends on the careful calculation of risk, then graduate education in that discipline is the currency of the future. DHS must support this effort.

3. **The education of senior executives in risk management is essential. Leaders will not support what they do not understand.** This education must be carefully tailored and presented to advance their knowledge while respecting their time. Leaders will embrace risk thinking when they are convinced that this new approach will solve their problems and not add to their burdens.
4. **Basic online training programs should be prepared for employees already working in the field of risk management across the homeland security enterprise.** Current FEMA courses (learnaboutrisk.org) are a great start—challenging, thorough, and suitable for a general audience. They should be expanded and targeted at senior executives and junior analysts in government as well as businesses and local jurisdictions. If we train just the executives, then the lower level staffers will not know how to do the work. If we train just the low-level staff, then the risk work will not get done because executives will not consider it worth the time of their subordinates. Therefore, courses for the nonprofessional, concurrent-duty, on-the-job trainee are needed in parallel to executive education about risk. This is a standard force development model that many large corporations and the U.S. military use.
5. **DHS must produce its own risk management education and training materials.** Given the broad range of institutions that use differing risk language and concepts, DHS will find that it cannot depend solely on contractors who learned their risk skills elsewhere. DHS needs DHS-related materials, with DHS-specific examples and case studies—related to the national preparedness system, if possible. As with the studies by the National Research Council and the IBM Business Group, the Risk Management Curriculum Review has already plowed this ground.⁷⁴ DHS should adopt those recommendations—doing the following, for example:
 - Build online games with the training so participants can learn by trial and error.
 - Build a separate game/education block for how to use risk quickly in a crisis.
 - “Firewall” the risk education/training program from existing bureaucracy. It is the well established nature of bureaucracy – all bureaucracy -- to protect itself and its programs. Many individual parts of DHS have now established their own Risk Management programs, complete with individual visions,

⁷⁴ Tanner, vi-vii; 9-13. This conference and follow on document produced by the DHS Chief Learning Office examined the existing curriculum for current internal DHS education and training programs. Essentially it evaluated what DHS is teaching its own people. Note especially the recommendation on what DHS employees at different levels need to know about risk.

objectives, training programs, etc. Positions and careers are now connected to these disparate programs. Left to their own devices, some of these organizations will attempt to absorb or undermine any competing vision, even if it is conceived as an overarching vision from the top. Any new competing DHS wide effort of this nature will have to be protected and directed by senior leadership or it will flounder. This is not to cast aspersions on any of the hard working, dedicated people in the Department of Homeland Security. This is simply an iron law of bureaucracies.

6. **Coordinate educational efforts, whenever possible, with universities and educational institutions.** This will give the risk management program an academic legitimacy that other internal DHS educational and training programs will have to respect. The following expound on this recommendation:
 - The starting point for this effort should be the Naval Postgraduate School, which has already developed risk-related curriculum and is ready to share it with academic partners, students, and alumni across the homeland enterprise nationwide.
 - The Homeland Security and Defense Education Consortium Association will be eager to act as a liaison to encourage teaching risk in more than 300 schools with homeland security programs, and will presumably profile the subject at their annual conference.
 - The U.S. Northern Command, DOD's primary operator for homeland security, has long had an active role in crossing the educational boundary between DOD, DHS, and civilian universities. They also help to sponsor an annual conference on homeland security issues, and will likely support teaching the new importance of risk management.
 - The Homeland Security Policy Institute at George Washington University has a program of lectures, conferences, and workshops on key homeland security issues that are recognized nationwide. They have special access to the think-tank community and should be contracted to present a series of activities promoting the importance of risk in DHS and homeland security activities writ large. As an independent academic organization, they can address what DHS has done right, where DHS has fallen short, and how the best concepts and practices in the field can be promoted across the entire homeland security enterprise.
7. **Ensure that both online and on-site training programs are made available through the FEMA Emergency Management Institute (EMI) website and the associated website for FEMA's higher education.** Create and deploy teaching and assistance teams to deliver a uniform understanding of risk within DHS agencies everywhere and across the enterprise as a whole. (This can be addressed by the Homeland Security Consortium based in Anniston, Alabama, at Louisiana State University, at Texas A&M University, etc.) This is the way other

essential information has been distributed (like the National Response Framework). Training on risk is just as important.

8. **Ensure that in creating curriculum and training/education teams, special attention is paid to**

- interaction with the intelligence community,
- risk communication, and
- incorporation of risk lessons into exercises.

THE CULTURE OF RISK MANAGEMENT

Senior leadership in DHS can implement all of the recommendations in the preceding sections. However, none of those recommendations will stay in force unless the DHS culture changes to accept them as the normal way of doing the business of risk management.

Institutional culture is the most powerful tool any institutional leader can have—or the greatest opponent. From a business perspective, “Culture is the pattern of shared beliefs and values that provides the members of an organization rules of behavior or accepted norms for conducting operations.”⁷⁵ In its simplest terms, culture is what the staff does when the boss is not present. When you hear an experienced employee tell a newcomer, “That’s how we do it here,” you know you have found the institution’s culture.⁷⁶

How then does DHS go about creating a risk management culture?

Observations: On the Problem of Establishing a Risk Management Culture

The department cannot create a new culture by directive or management. A directive simply tells people what to do; it does not convince them to internalize a new way of thinking and acting. The second approach, management, is the least likely way to promote a new culture of risk management. By definition, management is about keeping current practices operating smoothly in the current way.

Incorporating risk management into DHS culture will require a significant change in thinking. Change requires *leadership*, not management.

Changing the way people think in government is especially difficult, because so many senior leaders are political appointees who stay for a relatively short period of time. They frequently arrive with new ideas and new programs that disappear when their term is up. In examining a similar challenge in changing the culture of public health, Dr. Leslie Beitsch noted, “health veterans can recall numerous failed ‘new’ proven methods introduced during the course of their careers. More cynically, these fads represented the ‘flavor of the month,’ and were introduced by well-intended but naïve past administrations. Even when the ideas had genuine merit, resistance to change throughout the organization crippled implementation.”⁷⁷

⁷⁵ Vincent Omachonu and Joel Ross, *Principles of Total Quality* (CRC Press, 2004), 30.

⁷⁶ John Kotter, *Leading Change* (Harvard Business School Press, 1996), 20.

⁷⁷ Leslie Beitsch, “Performance Management in Action – The Role of Leadership,” in *The Public Health Quality Improvement Handbook*, (Milwaukee, WI: ASQ Quality Press, 2009), 283-284.

Recommendations: Some Ways to Promote a Culture of Risk Management

Major cultural change requires planning and leadership. Here are some successful approaches that DHS leadership might apply to the department.

Some Expert Advice

Perhaps the most successful path to culture change in modern history—and in some places the most reviled—is the Deming Method. Edwards Deming was the expert in quality management who revolutionized Japanese industry by identifying customer satisfaction as the first goal, and then focusing everyone in the company on that goal. New ways of thinking and new cultural norms included the following:

- Understanding that each person’s job was to contribute to the whole success, not compete with others to satisfy an internal standard;
- Recognizing that input from low-level staff and operators “where the rubber meets the road” might be more important than input from ranking supervisors, and
- Training and retraining, rather than blaming and removing.⁷⁸

Unfortunately, some government agencies applied the Deming Method poorly during the 1990s, “poisoning the well” for anyone who wants to apply the method to other government projects. Still, the example is so well known and successful that it should be considered by anyone looking to institute culture change into a large organization. (See annex B for central elements of the Deming Method.)

Perhaps a better starting point for the purposes of this paper is John Kotter, whose book on *Leading Change* has been leading management reading lists for 15 years. Kotter has identified the fundamental steps required to institutionalize change in most major organizations. DHS could adapt his “eight-stage process” to the challenge of making risk management a part of DHS culture.⁷⁹ A simplified list of Kotter’s process is below.

- Establish a sense of urgency.
 - Include crises, potential crises, and opportunities.
- Create a guiding coalition.
 - Charge a group with power to push the change as a team

⁷⁸ Mary Walton, *Deming Management at Work* (New York: Perigee Press, 1990). While Deming himself published a number of books, this book offers one of the most concise versions of his work—with examples.

⁷⁹ Kotter, 20.

- Develop a vision and strategy.
 - What does success look like? What path will get the organization there?
- Communicate the vision and the change required.
 - The actions of leaders speak louder than their words.
- Give people in the system the power to make the changes work.
 - Find out what gets in the way of risk management, and get rid of it.
- Plan for some short-term wins.
 - Show examples of successes and give credit where it is due.
- Leverage these gains to encourage more change.
 - Use the credibility gained to repeat the success.
- Anchor the changes into the long-term culture.
 - Do this by planning for succession.

This staged process appears tailored for incorporating risk management into the national preparedness system. Here are Kotter's eight stages again, refocused on inculcating risk management into the culture of DHS.

Establish a Sense of Urgency

This step has already been addressed within DHS by President Obama's signature on PPD-8, directing that DHS calculate and address "the greatest risks to our national security." Urgency is established within the broader homeland security enterprise by the requirement that DHS use risk management for FEMA grant requests.

Create a Guiding Coalition

DHS has addressed this step by creating the Risk Steering Committee. A remaining requirement is for the department's principals to take the lead from staffers who have been doing the job without the authority to make their changes stick.

Develop a Vision and Strategy

DHS has not completed this step. PPD-8 and published DHS policies previously cited in this paper lay out the vision to be achieved, and major steps to be taken (e.g., publishing a national risk assessment). The major requirement remaining is for the Office of Risk Management and Analysis to work with the National Protection and Programs Directorate and FEMA to generate a couple of quick case studies that demonstrate how risk to the nation was properly identified, analyzed, assessed, and managed. Such illustrations might enable others to envision clearly how the new process should work.

Communicate the Vision and the Change Required

This requires the Secretary of Homeland Security's personal attention. Her speeches, her meetings, and her travels need to show a personal interest in establishing risk management as "how we do it here."

Give People in the System the Power to Make the Changes Work

When the Secretary incorporates the ninth part of recommendation 4 (requiring briefings on improvements to the Quadrennial Homeland Security Review to be set in terms of risk management), she should ask for examples of how lower level staff and operators were included in the risk management process. DHS should then publicize them.

Plan for Some Short-Term Wins

DHS could easily accomplish this by using the national risk assessment (see recommendation 1) during preparations for the National Exercise Program, then publicizing the successful examples. Additionally, the pending use of risk management by DHS Science and Technology to prioritize program selection for budgeting will be seen as a major cultural and procedural change by participants across the entire homeland security enterprise.

Leverage These Gains to Encourage More Change

DHS can show the importance of risk management to the entire homeland security enterprise by using risk management wherever possible during the budget process for fiscal year 2013. Risk management, the National Risk Assessment, and the National Preparedness Program should then become the basis of budget priorities for 2014.

Anchor the Changes Into the Long-Term Culture

Applying risk management to the 2013 and 2014 budgets will ensure it is used for reporting to Congress at least twice. Once Congress gets used to relying on this information and process, it will serve to ingrain it into the DHS organizational ethos.⁸⁰

Lead From the Top

In organizations, people follow most closely what the boss does, not just what the boss says. Consequently, here is the most important single fact about establishing a risk culture at DHS: **risk will be incorporated into DHS daily operations and long-term planning and budgeting if the Secretary of Homeland Security practices it in the main office, and demands it of the senior staff.**

⁸⁰ In John Kotter and Lorne Whitehead, *Buy In: How to Keep Your Good Idea from Getting Shot Down* (Boston, MA: Harvard Business Review Press, 2010), 84-85, Kotter suggests 24 reasons commonly used to fight change and cultural adaptation. These objections should be expected by anyone trying to inculcate risk management into DHS culture. See them all at Appendix B.

If the system is left to change itself and to assimilate risk lessons and ideas on its own, no significant change will take place. People will take a narrow perspective and continue to do what seems to work and serve their own interests best. If a new idea is important enough for important people (which is to say bosses at the highest level) to adopt it, then subordinates will perceive it as important enough for their own attention. But limited commitment at the upper levels will translate to no commitment at the lower levels.

An efficient way for the Secretary to demonstrate her own interest in institutionalizing risk management would be to require that agencies already tasked with reporting their progress toward the five goals set in the Quadrennial Homeland Security Review couch their responses in risk management terms. Once the senior leaders in the department begin discussing the department's most important priorities using new risk language and frameworks, significant use of risk management will follow.

FINAL THOUGHTS

The United States has entered a difficult period in its history. For the foreseeable future it will be both at war and under considerable financial pressure. Safety and security must be paired with efficiency and effectiveness. One way to do this in the field of homeland security is through the application of risk management, integrated across the entire enterprise, as part of a “whole of nation” effort.

This white paper has examined the longstanding DHS attempt to do so, with the goal of applying a new strategic perspective to this enduring issue. The result has been a set of observations offered in five areas—reiterated further below—with accompanying recommendations associated with each.

Additional thoughts and recommendations offered by those the author interviewed are provided in a less structured form in Appendix D.

In short, the author concludes that the foundation work in risk done thus far by dedicated staff across two presidential administrations has been useful and worthwhile, but has fallen short of the national-level expectations repeatedly set for it. A number of good programs are underway, and many DHS agencies are beginning to employ compatible terms, concepts, and models. But one of the most important objectives has not been reached: efforts have not matured to the point that decisions, policies, operations, and acquisitions are routinely informed by a common approach to risk management. The failure to develop a bottom-up risk assessment is especially disappointing, since so many senior-level decisions should be informed by that document.

Furthermore, the author concludes that, despite improvements on the horizon, the effort will continue to fall short of expectations. The author therefore offers recommendations to address the shortcomings in five areas:

1. “Re-looking” at the application of risk management to address the most significant maximum-of-maximum concerns.
2. Rethinking the language to emphasize the positive goal of increased security rather than the negative goal of risk mitigation.
3. Revising the development and use of risk tools to provide decision makers a broader range of information, with a lesser chance of oversimplification and overconfidence.
4. Refocusing and reinvigorating efforts to promote staff professionalism in this field, to include the education and training required to support the use of risk thinking at every level—from occasional user to government and private executive.
5. Renewing the dedication of senior leaders to inculcating integrated risk management into the culture of the department and the enterprise nationwide.

These changes, with their strategic-level, long-term impact, are all achievable. At a time when so many government challenges and solutions seem difficult, expensive, or politically daunting, these recommendations are all practical, appropriate, comparable, transparent, and defensible—precisely in accordance with the risk management principles laid out in the integrated risk management framework.⁸¹

⁸¹ *Interim Integrated Risk Management Framework*, 6-7.

APPENDIX A – KEY DEFINITIONS

Key definitions for terms frequently used in this paper are listed below. All risk-related definitions are drawn from the DHS *Risk Lexicon*.

RISK:

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

Sample Usage: The team calculated the risk of a terrorist attack after analyzing intelligence reports, vulnerability assessments, and consequence models.

Extended Definition: potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence

Annotation:

1. Risk is defined as the potential for an unwanted outcome. This potential is often measured and used to compare different future situations.
2. Risk may manifest at the strategic, operational, and tactical levels.
3. For terrorist attacks or criminal activities, the likelihood of an incident, event, or occurrence can be estimated by considering threats and vulnerabilities.

RISK ANALYSIS:

Definition: systematic examination of the components and characteristics of risk

Sample Usage: Using risk analysis, the community identified the potential consequences from flooding.

Annotation: In practice, risk analysis is generally conducted to produce a risk assessment. Risk analysis can also involve aggregation of the results of risk assessments to produce a valuation of risks for the purpose of informing decisions. In addition, risk analysis can be done on proposed alternative risk management strategies to determine the likely impact of the strategies on the overall risk.

RISK ASSESSMENT:

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

Sample Usage: The analysts produced a risk assessment outlining risks to the aviation industry.

Extended Definition: appraisal of the risks facing an entity, asset, system, network, geographic area or other grouping

Annotation: A risk assessment can be the resulting product created through analysis of the component parts of risk.

RISK MANAGEMENT:

Definition: process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken

Sample Usage: The organization employed risk management to understand and reduce the risk it faced.

Annotation: Effective risk management improves the quality of decision making. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to control risk.

INTEGRATED RISK MANAGEMENT:

Definition: structured approach that enables the distribution and employment of shared risk information and analysis and the synchronization of independent yet complementary risk management strategies to unify efforts across the enterprise

Sample Usage: DHS uses an integrated risk management framework to promote a unified approach to managing all homeland security risks.

RISK-BASED DECISION MAKING:

Definition: determination of a course of action predicated primarily on the assessment of risk and the expected impact of that course of action on that risk

Sample Usage: After reading about threats and vulnerabilities associated with vehicle explosives, she practiced risk-based decision making by authorizing the installation of additional security measures.

Annotation: Risk-based decision making uses the assessment of risk as the primary decision driver, while risk-informed decision making may account for multiple sources of information not included in the assessment of risk as significant inputs to the decision process in addition to risk information. Risk-based decision making has often been used interchangeably, but incorrectly, with risk-informed decision making.

RISK -INFORMED DECISION MAKING:

Definition: determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, as well as other relevant factors

Sample Usage: He practiced risk-informed decision making in planning event security by considering both the results of the risk assessment and logistical constraints.

Annotation: Risk-informed decision making may take into account multiple sources of information not included specifically in the assessment of risk as inputs to the decision process in addition to risk information, while risk-based decision making uses the assessment of risk as the primary decision driver.

APPENDIX B – THE DEMING METHOD

The following is taken directly from Mary Walton's book on Deming management.⁸²

The Fourteen Points

1. Create constancy of purpose for improvement of product and service.
2. Adopt the new philosophy.
3. Cease dependence on mass inspection.
4. End the practice of awarding business on the price tag alone.
5. Improve constantly and forever the system of production and service.
6. Institute training.
7. Institute leadership.
8. Drive out fear.
9. Break down the barriers between staff areas.
10. Eliminate slogans, exhortations and targets for the work force.
11. Eliminate numerical quotas.
12. Remove barriers to pride of workmanship.
13. Institute a vigorous program of education and retraining.
14. Take action to accomplish the transformation.

The Seven Deadly Diseases

1. Lack of consistency of purpose.
2. Emphasis on short-term profits.
3. Evaluation by performance, merit rating or annual review of performance.
4. Mobility management.
5. Running the company on visible figures alone.
6. Excess medical costs for employee health care, which increases the final costs of goods and services.
7. Excessive costs of warranty, fueled by lawyers who work on the basis of contingency fees.

⁸² *Deming Management at Work*, 17-19.

This page intentionally left blank

APPENDIX C – REASONS PEOPLE OPPOSE CHANGE

Anyone who has ever tried to bring change to government will recognize these reasons that we cannot or should not change. Anyone trying to inculcate risk management into DHS or any other part of the national enterprise should be ready to argue them down.

(The following is taken directly from Kotter and Whitehead's book *Buy In: How to Keep Your Good Idea from Getting Shot Down*.⁸³)

1. We have been successful; why change?
2. Money (or some other point used to distract the argument) is the only real issue.
3. You exaggerate the problem.
4. You're implying that we've been failing.
5. What's the hidden agenda here?
6. What about this and that and this and that . . . ? (off-the-topic delay)
7. Your idea goes too far/doesn't go far enough.
8. You have a chicken-and-egg problem. (We can't get started.)
9. Sounds like [*something most people dislike*] to me.
10. You're abandoning our core values.
11. It's too simplistic to work.
12. No one else does this.
13. You can't have it both ways. (a reason not to do anything)
14. But you can't deny that . . . (some extraneous objection held to the last to distract)
15. If the idea generates this many questions and concerns—there must be something wrong.
16. We tried it before—it didn't work.
17. It's too difficult to understand.
18. Good ideas, but this is not the right time.
19. It's too much for our team.
20. It won't work here because we are different.
21. It puts us on a slippery slope.
22. We can't afford this.

⁸³ *Buy In*, 84-85.

23. You'll never convince enough people.
24. We're simply not equipped to do this.

APPENDIX D – COMMENTS FROM INTERVIEWS AND REVIEWS

Note: In the preparation of this white paper the author was struck by the absolute lack of political or partisan rhetoric from those he interviewed. People, both inside and outside of the government, want to get homeland security right. Here are some interesting thoughts contributed during those interviews. Some agree with the ideas suggested in the main body of this white paper; some disagree. But all were made in the spirit of trying to improve the way that risk serves the safety and security of the United States. In accordance with the rules of the interviews, no names are attached to these observations.

----- Comment 1

Consider how the United States Northern Command and Defense Support to Civil Authority (DSCA) fit into the concepts and calculations of risk management.⁸⁴ It is very hard to write DOD forces into the role of reducing vulnerabilities, since DOD resources are committed primarily on an “as needed” basis. But their activities should be included as part of the risk calculation for consequence management, especially for maximum of maximums that endanger the nation as a whole.

----- Comment 2

A major challenge is people “gaming the system” for additional resources. Is DHS really going to accept whatever approach to risk assessment the grant applicants want to offer? (This suggestion is repeated several times in the FEMA educational product, learnaboutrisk.org). Should not FEMA/DHS establish a process of approving approaches to risk assessment? Such enterprise-level common guidance will be essential to promote honest analysis and high confidence in results.

----- Comment 3

Concerning the language of risk, begin talking about risk management as outcome management—then consider incentives to promote adoption of paths leading to the desired outcome.

----- Comment 4

Risk language today seems focused on risk to critical infrastructure and key resources. As DHS doctrine matures, it needs terms to talk about an expanded list of types of risk. For example, DHS should consider:

⁸⁴ NORTHCOM is the joint military command that oversees the preparation and employment of Department of Defense resources to conduct and support the homeland security mission within the confines of the United States. DSCA is the way the mission of homeland security is generally described within DOD. The terminology emphasizes that, by doctrine, DOD never has the lead in such plans and operations.

- Technical risk (consider: if accomplished, would the outcome be adequate, achievable, acceptable, sustainable)
- Programmatic risk (consider: cost vs. benefit, cost vs. schedule vs. /Quality Cheap-Fast-Good)
- Human capital risk (consider: how to prevent getting the wrong person with the wrong skills in the wrong job).

----- **Comment 5**

When using the traditional equation **risk = threat x vulnerability x consequences** to prioritize resources, we generally explain quite clearly how reducing “T” or “V” or “C” reduces “R.” But we frequently miss the fact that reducing any of the three variables may reduce the other two variables as well. For example, the action that reduces consequences will also make the target less inviting, and thereby reduce threat as well. The same action may also reduce vulnerability.

So...if C and V and T are all reduced by the same action, then the change in R is going to be much larger than if C were reduced by its self.

----- **Comment 6**

Not everyone agrees with the approach that calculates the risk from terrorists and natural events the same way. There is a political dynamic to a terrorist attack that is missing from natural disasters. That dynamic—having to do with the loss of legitimacy by a government unable to stop attacks—is not adequately captured by “consequences.” Thus terrorist attacks have a greater impact on national security by definition, and should be listed and evaluated separately from natural disasters.

----- **Comment 7**

Success is influenced more by leadership than plans. Leadership is greatly influenced by training. Adequate training must be based on real-world lessons learned. The risk management process and diagram should specifically mention the necessity for continuous senior leader training and education. Unless it is systematically required and checked, it will not happen.

----- **Comment 8**

For clarity and impact it is worth restating a major point of recommendation 2. In order for risk management and expenditure prioritization to work enterprise-wide, a common language is required between federal, state, local, private, international, and nongovernmental organizations and people. Traditional terms associated with *risk* and *risk management* are already used in multiple ways by other organizations. We need a different vocabulary from the risk vocabulary already in use.

----- **Comment 9**

The economic and financial worlds do not have any monopoly on the use of either the language or the concepts inherent in risk management. A bigger current problem than

confused language is a tendency for risk analysts to develop an approach that works for one problem and demand that it be applied universally. We should move to address this problem, rather than giving up on risk language and concepts as a whole.

----- **Comment 10**

“Risk management” is more than merely a planning process or a management activity. It is actually a very high-level strategy in and of itself. Risk management involves actions taken to reduce the likelihood of something bad happening (i.e., prevention) and actions taken to reduce the harm suffered when prevention fails (response and/or consequence management). Thus, risk management satisfies the current DOD definition of “**strategy**—a prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives.”⁸⁵

----- **Comment 11**

One of the issues affecting the utility of the risk management notion is that there is no single organization for risk managers but there is just such a single body for risk analysts (Society for Risk Analysis – www.sra.org) This organization is almost singly focused on issues surrounding the analysis of risk. While SRA does have a number of specialty groups within it, the focus is on analysis rather than on the management of risks. The positive aspect of this is that it advances the practice of risk analysis. The negative aspect is to skew attention within DHS away from the larger body of work encompassed within “risk analysis.”

----- **Comment 12**

One of the biggest problems of risk management in DHS has been the failure to adapt concepts to the characteristics of the homeland security problem space, resulting in improper calculations. In normal risk management, as with the case of exploding marine boilers, the solutions (e.g., adequate design standards) had to be applied to every boiler because every boiler that was not adequately designed and built was going to explode. In terrorism, not every unprotected target will be attacked. Thus, adding the calculated risks for every potential target in a given class, which would be appropriate for traditional industrial safety risks, gives you a risk figure that is grossly disproportionate to the actual risk.

⁸⁵ U.S. Army, **Field Manual 3.0, Change 1, Chapter 7, Paragraph 7-10** (Washington, DC: Headquarters, Department of the Army, February 22, 2011), <http://www.fas.org/irp/doddir/army/fm3-0.pdf>. (An alternate site for just chapter 7: <https://rdl.train.army.mil/soldierPortal/atia/adlsc/view/public/11636-1/fm/3-0/chap7.htm>.)

----- **Comment 13**

Over a long career in risk management, here is a list of some of the problems repeatedly encountered in the field:

- Unrealistic promises made by “risk analysis experts” about the ability of their process to give definitive, highly reliable answers
- Unrealistic expectations, spurred on by unrealistic promises
- Managers who see risk management as a number generator that will reduce their personal risk in decision making
- Risk assessment being pursued as individual projects rather than as an effort to generate coordinated decision-support information

----- **Comment 14**

Not everyone who works in risk management agrees with the formula $R = T \times V \times C$. Some see this “equation” more as a metaphor or perhaps a mnemonic that aids in conceptualizing the functions and relationships without trying to imply causal effect or quantifiable outcomes or elements. In fact, emphasis on the word “calculate” and all of its various derivatives is part of the problem: some people are demanding rigorously calculated numerical answers to questions for which such answers are meaningless. Of course the problem here is that some in DHS are looking to risk management precisely for the purpose of generating defensible calculations to prioritize expenditures.

----- **Comment 15**

Concerning implementing a risk culture in DHS, the most important thing required is a mandate with teeth. The Secretary of Homeland Security needs to put requirements for progress in this area, into her direct-report staff’s performance agreements, and then hold people accountable, not just for action but for the right actions.



HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

An FFRDC operated by Analytic Services Inc. on behalf of DHS

2900 South Quincy Street • Suite 800 • Arlington, VA 22206-2233