SANDIA REPORT
SAND2008-7828
Unclassified – Unlimited Release
Distributed December 2008

Homeland Security R&D Roadmapping – Risk-based Methodological Options

Larry D. Brandt

Prepared by
Sandia National Laboratories
Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

SAND2008-7828
Unclassified – Unlimited Release

Homeland Security R&D Roadmapping –

Risk-based Methodological Options

Larry D. Brandt

Sandia National Laboratories
P.O. Box 969
Livermore, CA 94551-0969

Abstract

The Department of Energy (DOE) National Laboratories support the Department of Homeland Security (DHS) in the development and execution of a research and development (R&D) strategy to improve the nation's preparedness against terrorist threats. Current approaches to planning and prioritization of DHS research decisions are informed by risk assessment tools and processes intended to allocate resources to programs that are likely to have the highest payoff. Early applications of such processes have faced challenges in several areas, including characterization of the intelligent adversary and linkage to strategic risk management decisions. The risk-based analysis initiatives at Sandia Laboratories could augment the methodologies currently being applied by the DHS and could support more credible R&D roadmapping for national homeland security programs. Implementation and execution issues facing homeland security R&D initiatives within the national laboratories emerged as a particular concern in this research.

Foreword

The work documented in this report was supported by a “late-start” LDRD grant in the summer of 2008. The conclusions documented here flowed from a short (~ 1 man month) effort executed at the end of summer 2008. Because of the limitations in time and resources, the resulting conclusions draw heavily from work of others in the risk assessment and risk management disciplines. This work offers primarily an integrating perspective and critical review of current approaches. As the national laboratories are heavily committed to technology development and application in risk-based decision making, it is hoped that some of the themes identified here can be further developed in larger, future projects.

Contents

Figures

This Page Intentionally Blank

Homeland Security R&D Roadmapping –

Risk-based Methodological Options

1. Introduction

The Department of Homeland Security (DHS) has responded to national policy mandates by extensive efforts to adopt risk-based planning as the foundation for resource allocation and strategic decision making. [1] The DHS Science and Technology (S&T) Directorate faces particularly daunting challenges in its research and development (R&D) preparations for Weapons of Mass Destruction (WMD) attacks. This is due the complexities and large uncertainties in the threat, attack scenarios, and response effectiveness for WMD events.

The Department of Energy (DOE) national laboratories, and Sandia National Laboratories in particular, have made significant investments in the development of risk-based methodologies to guide government decisions and technical system designs. These advances began with assessments addressing nuclear energy and nuclear weapons design and operations, and have broadened to include a diverse array of national and homeland security problem areas. Within Sandia's homeland security program, significant discretionary resources have been applied to problems of risk assessment and risk-based decision making.

This LDRD project sought to identify ways in which advanced risk management methodologies could be applied by the national laboratories to improve DHS efforts to define and execute R&D decisions that will provide the greatest benefit to the nation's homeland security preparedness against WMD attacks. To that end, an initial review of DHS S&T risk-based assessments was completed to understand the strengths and shortcomings of current methodological approaches. Then, an assessment of emerging methodologies (emphasizing those under development at Sandia Laboratories) was pursued to identify attributes of those research areas that might address the gaps in currently employed processes. Finally, recognizing that real impact on the security posture of the nation can occur only when plans are implemented, the work addressed potential barriers to national laboratory execution of the recommended methodologies and resulting roadmaps.

Limitations in the duration and depth of this research restricted the range of new methodologies surveyed, and precluded the application of the recommended improvements to an R&D planning example. However, the insights developed here will hopefully provide a starting point for further work in this area.

[1] The Homeland Security Presidential Directive – 10 (HSPD-10) established a requirement for a Biological Threat Risk Assessment to serve as a focal point for the development of a national biodefense strategy. This requirement was extended to all WMD attack modalities (biological, chemical, radiological, and nuclear) by HSPD-18.

2. Context and Approach

2.1 Current Approaches

Current technical approaches to risk assessment in homeland security programs build upon the tradition of probabilistic risk assessment (PRA) methodologies pioneered for nuclear reactor accidents and broadly applied to diverse technical problems since. The overall field of risk-based analysis might be broadly divided between risk assessments and decision analyses. Risk assessments seek to define a probabilistic outcome metric over a set of future uncertain events of interest, drawing on both classical statistical data and Bayesian estimates for the underlying sources of uncertainty. Decision analyses incorporate the impacts of alternative courses of action into the probabilistic model, allowing the setting of decision variables during the computational process in a manner that optimizes the chosen probabilistic metric. Linkage with implementation is improved in a well structured decision analysis, where the modeled decision variables are tied to factors under the control of the decision maker. The review in this report focuses on probabilistic risk assessment since these processes have been central to current DHS applications.

There are many risk and vulnerability assessment tools currently in existence. The number and use of these tools has grown dramatically since the events of fall 2001. Risk and vulnerability assessment tools have increasing been employed by owners of critical infrastructure facilities to identify and prioritize investments in vulnerability reduction.[2] Applications to homeland security R&D strategic program planning are more challenging. In this arena, several major risk assessment efforts (particularly those mandated by HSPD-10 and HSPD-18) have been pursued to inform managers of large DHS WMD defensive programs.

The shortcomings of the traditional PRA-based methodologies have caused some reviewers to recommend a broader risk management perspective be incorporated into high level planning processes. In one review[3], the U.S. Government Accountability Office (GAO) postulated the high level risk management framework shown in Figure 1. While this framework does not provide substantial technical detail, it does highlight areas that are often cited as shortcomings of current methodologies – specifically, addressing real decision alternatives and including implementation as a critical step in the analysis. This is a point that is re-emphasized by the research findings in this report.

[2] The tools and processes required for a focused infrastructure risk assessment embody some of the same principles as the larger DHS strategic assessments. HSPD-7 indicated that risk-based analysis should be employed to guide critical infrastructure protection. A number of approaches have been developed to guide vulnerability reduction decisions by infrastructure owners (see, for example, Risk Analysis and Management for Critical Asset Protection – RAMCAP. http://www.asme-iti.org/RAMCAP/)

[3] "Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure", U.S. Government Accountability Office, Report GAO-06-91, December 2005. A similar perspective is repeated in "Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security", U.S. Government Accountability Office, Testimony GAO-08-904T, June 2008.

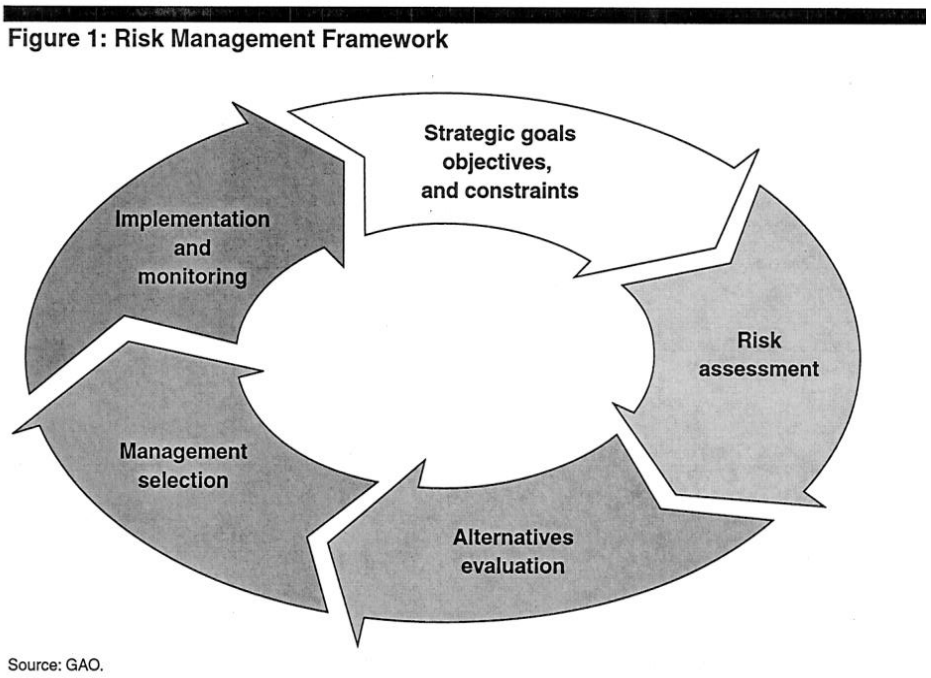

Figure 1. Risk Management Framework

2.2 DHS Biological Risk Assessment – An Exemplary Case

The application of risk assessment processes to strategic program decisions has been pioneered within DHS S&T by the biological countermeasures program due, in part, to the mandate of HSPD-10. The 2006 Bioterrorism Risk Assessment[4] (BTRA) is analyzed here as a baseline to provide input regarding the strengths and weakness of the methodology that has been developed by DHS for their WMD risk assessments. The National Research Council (NRC) Committee on Methodological Improvements to the DHS Biological Agent Risk Analysis was also convened to evaluate the methodology employed in the 2006 BTRA. Several national laboratory researchers who played key roles in the 2006 assessment and subsequent DHS risk assessment work were also contacted to substantiate available written documentation. Extensive risk assessment work has occurred within DHS subsequent to the completion of the 2006 BTRA. An updated 2008 BTRA is in process. In addition, an "all-WMD" risk assessment is near completion in response to the requirements of HSPD-18. Based on discussions with participants, the more recent processes share a similar approach and toolset that was originally employed for the 2006 BTRA. Hence, the comments included in the following sections are expected to be largely valid for assessments currently in progress.

[4] While the findings of the 2006 BTRA remain classified and hence generally unavailable to the open research community, the unclassified methodology sections were reviewed to provide input to the conclusions in this report. A detailed summary of the methodological approach can be found in the National Academies Press reports referenced below.

The 2006 BTRA had as its principal goal the prioritization of candidate bioterror agents based on a probabilistic risk assessment that considered a wide range of terrorist scenarios. The level of human fatalities was the metric. A standard event tree structure was established that included the major phases of the attack (e.g., agent acquisition, production, dissemination, transport, infection, …). Subject matter experts (SMEs) and intelligence community analysts provided the prior probability distributions over the parameters that specified the attack characteristics and adversary choices. The identification of those event tree parameters that strongly affected the probability or consequences of an event provided decision makers with a perspective on which areas were most important to address in program decisions aimed at risk reduction. However, uncertainties associated with the performance of future candidate defensive systems were not explicitly evaluated.[5] Critical knowledge gaps for uncertain scientific phenomena that significantly affect consequences were also identified. Informal feedback on the process from participants highlighted the learning value resulting from convening the nation's key subject matter and intelligence experts to inform DHS participants regarding the critical factors influencing the likelihood and consequences of a biological attack. The relative ranking of threatening agents provides one basis for guiding program decisions. In addition, the extensive reference library generated during the process could provide the diligent DHS staffer with a broad array of technical inputs that could influence program decisions.

The review of the methodology by the NRC Committee on Methodological Improvements to the DHS Biological Agent Risk Analysis[6] provided an independent perspective on the shortcomings of the current methodology. Their three principal interim recommendations were:

- *DHS should establish a clear statement of the long-term purpose of its bioterrorism risk analysis.*
- *DHS should improve its analysis of intelligent adversaries.*
- *DHS should increase its risk analysis emphasis on risk management.*

The first and third findings reflect a key theme of the NRC review. They were particularly concerned that the assessment process and outcomes provide a means to impact risk management decision making. There is no methodological component in the current process that addresses how changes in specific investments translate into changes in risk. Furthermore, while the participants in the process likely gained important insights into the critical risk parameters, there was no easily accessible tool that could be employed by other program managers or concerned government personnel to understand the implications of the assessments on their own areas of responsibility. Both of these findings underscore the earlier discussion from GAO regarding the importance of linking probabilistic assessments to alternative selection and implementation. The second finding regarding intelligent adversaries indicates that the traditional, event tree, PRA-based approach that has worked so well for physical systems (e.g., nuclear reactor accidents),

[5] Feedback from participants in the 2008 process indicated that national systems deployed to respond to biological attack were modeled as a part of that recent assessment. Most notable among these are the BioWatch detection system and the Strategic National Stockpile for post-event medical treatment.

[6] The interim report of the committee was documented in "Interim Report on Methodological Improvements to the DHS Biological Agent Risk Analysis", National Academies Press, 2007, (http://www.nap.edu/catalog.php?record_id=11836). The final report is available as "Department of Homeland Security Bioterrorism Risk Assessment: Call for Change", National Academies Press, 2008, (http://www.nap.edu/catalog.php?record_id=12206).

needs modification for intelligent adversaries. The decision calculus of a real adversary will likely include assessment of the likelihood of success, as well as numerous provisions for responses to unexpected defensive measures and operational outcomes. In addition, elicitation of event tree probabilities cannot effectively capture the value assumptions behind an adversary's decision to proceed with a WMD attack. All of these factors argue for a more sophisticated treatment of adversary behavior within the risk assessment process.[7]

2.3 Gaps and Shortfalls in Current Methodologies

The review of the 2006 biological assessment, supported by consideration of more recent, related DHS efforts, has provided a basis for a critique of the current risk-based approaches to this problem. The DHS process responded to policy mandates to examine the overall WMD threat, attack, and consequence environment. The resulting process and product were the first steps in rationalizing preparedness options for the federal, state, and local governments. However, the following appear to be areas in which the initial methodological approaches might be improved:

- Threat Assessment: The use of standard PRA techniques to assess the absolute likelihood of terrorist WMD events is likely to be misleading. An intelligent adversary will seek to evaluate the expected success and impact of his attack, and make decisions that will address his value objectives. Unconditional assessments that do not model the adversarial decision process, or account for vulnerability reduction or other defensive measures, will miss key elements that are critical to risk management decisions.
- Links to Risk Management Decisions: A fundamental difficulty of PRA processes for WMD terrorism assessment is linkage to risk management decision alternatives. While heuristic links and general insights by participants in the assessment process will occur, an approach to tie the work to a wider audience charged with the development and execution of relevant programs has not been developed. This is particularly the case for R&D options, which often have uncertain and cross-cutting outcomes.
- Consideration of non-WMD and Other Cross-cutting Benefits: Many elements of national preparedness are difficult to model within the context of a probabilistic risk assessment. Cross-cutting investments in the resilience of crisis response against diverse natural and terrorist threats will support many critical national missions, so their value should not be tied solely to WMD scenarios.
- Implementation of R&D Programs: The implementation of the insights from the probabilistic risk assessment framework depends on many factors outside of the realm of the assessment. Some of these issues, particularly as they apply to national laboratories decisions, were touched upon in this research.

It must be noted that several of the methodological issues outlined above are made more challenging due to the immaturity of strategic decision processes within DHS S&T. This is one of the factors that led portions of the research to address the problem from the perspectives of the national labs as key providers of R&D and strategic collaboration in support of DHS.

[7] A summary of the NRC committee recommendations can be found in Parnell, G.S. et al, "Scientists Urge DHS to Improve Bioterrorism Risk Assessment", Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, Volume 6, Number 4, 2008.

3. Pathways for Improvement

3.1. Categories for Review

It is useful to separate the shortcomings and concerns outlined above into two major discussion categories that encompass the prospective improvements that might be relevant. The first would identify how emerging methodological options could address the difficulties in the current probabilistic approaches. Central to this category would be considerations of appropriate treatment of threat and attack assessments, as well as the linkage to R&D strategies and their outcomes. The second would propose approaches to implementation that could allow the results of the assessments to be used more broadly to achieve real progress toward national preparedness. A particular focus of this second category is the role and responsibility of the DOE laboratories in determining and implementing homeland security options that will most effectively serve the national interest. Findings in each of these categories of investigation are summarized below.

3.2. Methodological Pathways

Some of the methodological difficulties associated with WMD risk assessments intended for strategic program applications stem from the employment of probabilistic approaches originally developed for physical system safety assessments. Such approaches require assessment of the unconditional probabilities of upset events, and models of the propagation of such events through the physical system (e.g., nuclear reactor core and containment) as well as subsequent environmental and human effects modeling. In these methodologies, the effects of physical system design changes can be easily incorporated into the analysis via appropriate sensitivity studies. For homeland security R&D decision making, the problems are significantly different. The nature of an attack depends on the current value metrics for the perpetrators and their perception of the vulnerability of their alternative targets. The real and perceived future vulnerability of various target options will be a complex function of the success and implementation details for various R&D options facing the U.S. The range of WMD approaches and target responses can be very large, with intangibles such as the resilience of U.S. response and changing risk perceptions following the event having major effects. Use of a traditional probabilistic risk assessment methodology can help program and policy decision makers understand the technical realities associated with a limited set of specific scenarios, but will not address these broader challenges associated with strategy development and implementation.

Sandia National Laboratories have allocated extensive efforts to the development of risk-based capabilities and their application to systems design. These capabilities were initially developed in the more traditional, safety-focused realms of nuclear reactor accidents and nuclear spent fuel storage. Extensions to areas where adversary capabilities and decisions are an important factor were pioneered for the physical security nuclear weapons and other critical national security assets. Two recent research initiatives within the laboratories dealing with the assessment and response to WMD homeland security threats address several of the shortcomings in the current DHS risk assessment processes.

The first of these Sandia initiatives is an internal research and development project that provides a more sophisticated model for threat assessment and permits iteration of the set of threat scenarios based on postulated defensive responses.[8] The study group recognized that the likelihood of an attack depended not only upon the capabilities of the perpetrators, but other factors that influenced expected attack effectiveness, including vulnerability of the target and both near and longer term consequences subsequent to the attack. Such a structure emphasizes the importance of considering outcome factors in addition to technical capabilities when assessing the actions of potential attackers. It also highlights the need to iterate assessments regarding threat likelihood when defensive decisions change target vulnerability and expected attack consequences. A fundamental decision calculus for modeling terrorist group behavior is illustrated in Figure 2. The research team has also developed an overall risk assessment protocol (termed "Total Risk Assessment") that provides a framework for explicit modification of the set of threatening scenarios based on assessment of both defensive measures that reduce vulnerabilities or response measures that impact consequences (e.g., infrastructure and social resilience factors). Such changes address the weaknesses of traditional probabilistic risk assessment structures in handling the interdependencies resulting from intelligent decision making by the adversary.

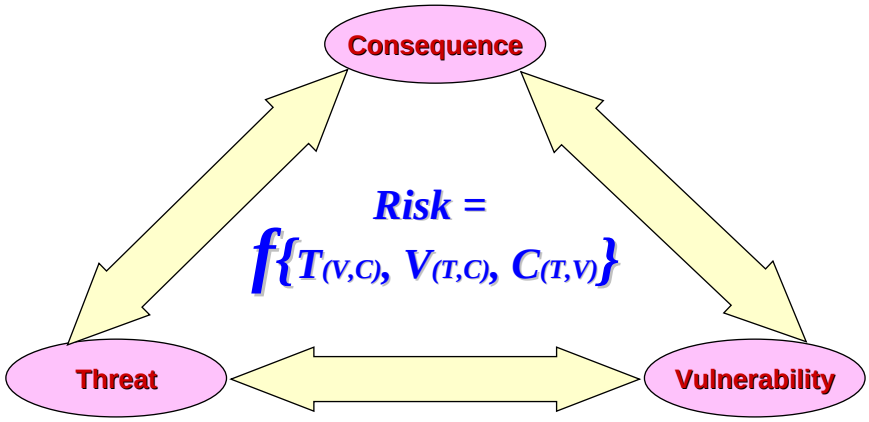

Figure 2. Interdependence of Key Assessment Factors for Malevolent Adversaries

Another recent capability development study, the Investment Planning and Analysis Tools (IPAT) project, was executed by a joint Sandia and University of New Mexico (UNM) analysis team for the Defense Threat Reduction Agency.[9] The work focused on assessing the impact of alternative procurement portfolios for chemical and biological defense assets using a risk-based measure of effectiveness. The initial effort integrated the UNM Risk Analysis Investment Decision Support (RAIDS) system with a Sandia modeling tool that supplies ground truth performance estimates for the biological scenarios and defensive deployments used in the analysis. The RAIDS methodology employs a series of micro-models to capture the dependence of the performance of the biological defense system on decisions in the investment portfolio.

[8] Wyss, Gregory D. et al, "Total Risk Assessment", Internal Sandia briefing reporting progress on Laboratory Directed Research & Development (LDRD) project, September 24, 2008, For Official Use Only. This work will be documented in a Sandia LDRD Report.

[9] "Risk and Consequence Management Analysis: An Integrated Decision Analysis Architecture with a Focus on Chem-Bio", Final project briefing presented to the Joint Science and Technology Office for Chemical and Biological Defense, U.S. Department of Defense, April 16, 2008, For Official Use Only.

This is approach is both a strength and weakness for the system. The strength is its ability to directly estimate the impact of investment decisions on risk-based performance measures – a goal that has been highlighted earlier in this report. The weakness of the micro-model approach, particularly as implemented in the current IPAT treatment, is the inability of those models to capture the interdependencies and subtle features of the diverse defensive architectures and concepts of operations (CONOPS) that result from different investment portfolio decisions. While this could be remedied by incorporating a higher fidelity simulation model directly into the investment tool, this would increase the overhead associated with development and use of the resulting overall package. In spite of some concerns regarding the validity of the internal performance modeling in IPAT, its emphasis on providing direct quantitative links between current decision variables and future, risk-weighted, performance estimates is a step towards more effective risk management. This kind of quantitative link between current investment decisions and future outcomes is particularly important when addressing R&D decisions that have very uncertain implementation and success trajectories.

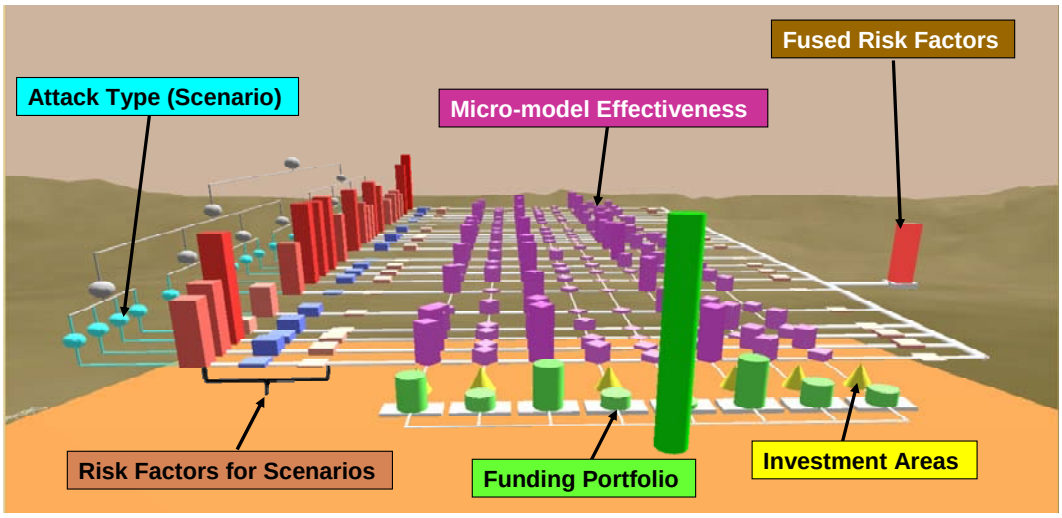

Figure 3. Analysis Flow for IPAT-RAIDS Methodology

These two recent research projects provide elements that address current concerns regarding national risk assessment processes. Other alternatives most certainly exist in the broader risk analysis community, and should be considered in any extension of this work. For example, existing approaches[10] for more narrowly prescribed problems may have elements that might also augment current processes.

3.3. Implementation Pathways

The methodological options examined above, as well as other risk-based engineering approaches, exist within Sandia and the other DOE national laboratories as a result of both fundamental research and the evolution of capabilities within applied national security programs. To achieve meaningful impact on DHS R&D road mapping and strategic decision making, these capabilities

[10] The infrastructure protection tools referenced earlier (e.g., RAMCAP) may contain notable features that could be incorporated in more strategic tools. The National Academies review of the 2006 BTRA process also provides a good starting point for future research in this area.

must be applied and influence the risk assessment and program management processes underway within the department. Discussions pursued as a part of this research indicated that this implementation phase was a critical gap for risk management methodologies, and also for a wider range of homeland security R&D technologies that are perceived by many at the laboratories to offer great future promise for homeland security advances. As a result of this feedback, a portion of the research effort was directed towards the analysis and development of recommendations regarding ways in which laboratories' capabilities could be more effectively linked to DHS R&D strategic decision making.

Groundrules for the employment of national laboratory R&D capabilities by DHS were originally addressed in the founding legislation of the department.[11] Subsequent negotiations with the DOE clarified the priority of the homeland security mission and developed administrative protocols by which the laboratories could work with DHS.[12] However, a GAO review indicated that the mechanisms in place for the effective employment of the labs (along with other national R&D resources) were inadequate.[13] A more recent government assessment[14] acknowledged the progress that DHS has made in placing an R&D management framework and strategic plan in place, but questioned the fundamental strategic resource allocation decisions. These are the decisions that the high level, risk-based, assessment methodologies reviewed in this research might impact.

The national laboratories have a strong record of accomplishment in the development and prototyping of advanced defensive systems to protect the nation against a terrorist WMD attack. Yet many at the national laboratories see the implementation and execution environment for DHS R&D initiatives as being a major barrier in the application of national laboratories capabilities. Factors cited for this perception include discontinuity and micro-management, reduced roles in the risk-based strategic priority setting, and inadequate investment in longer term research and capability development.[15]

One task within the current research effort was development of a national laboratory perspective on R&D implementation issues facing DHS. The findings from this work were documented in an unpublished white paper[16] that was coordinated among several of the national laboratories that execute R&D for DHS. The goal of the white paper was to combine available government documentation with insights from selected national laboratory personnel who have been key contributors to homeland security R&D over the last decade. The white paper noted the governmental comments from the GAO and CRS cited above. Evidence of exemplary programs

[11] Homeland Security Act of 2002 (H.R. 5005), Title III Sec. 309.
[12] "Reimbursable Work for the Department of Homeland Security", DOE Order N481.1A, Approved 4-21-2003. The underlying Memorandum of Agreement between the Secretary of Energy and the Secretary of Homeland Security, signed on February 28, 2003, is included as attachment 3 to this DOE order.
[13] "DHS Needs a Strategy to Use DOE's Laboratories for Research on Nuclear, Biological, and Chemical Detection and Response Technologies", U.S. General Accounting Office, GAO-04-653, May 2004.
[14] "The DHS Directorate of Science and Technology: Key Issues for Congress", U.S. Congressional Research Service, Report RL34356, February 1, 2008. The reviewers in this report indicated that congressional concerns regarding DHS S&T management of R&D programs had abated substantially since the GAO 2004 review. However, they cited other concerns regarding the relationship between the laboratories and private sector R&D suppliers in the execution of the DHS R&D portfolio.
[15] Some of these factors are also mentioned by government reviewers (e.g., CRS Rpt RL34356, 2008).
[16] Brandt, L.D., "Moving DHS R&D to the Next Level – A DOE National Laboratories' Perspective", Unpublished Sandia White Paper, September 30, 2008.

completed by the national laboratories, including technical reachback centers, BioWatch, special event protection against WMD attacks, transportation infrastructure protection, and WMD technical forensic analysis were discussed as examples of the capabilities of the national laboratories to link cutting-edge research with implementation. A number of factors were identified that have accounted for the historical accomplishments of the national labs in the implementation of high-impact, mission-focused, homeland security programs. These included:

- Early, high-level participation in program definition – The strength of the national laboratories can be best utilized by early participation in systems design and CONOPS development, and by engagement with the ultimate operators.
- Maintenance of a strong underlying technical base – The underlying research base at the national laboratories is essential to the provision of rapid, cost effective responses to homeland security challenges.
- Continuity of strategic objectives – Continuity of DHS R&D programs is needed to draw the best technical expertise and to permit year-by-year building of an experience base that can respond to new challenges and provide cost effective improvements in deployed defensive systems.
- Flexibility in program management – The national laboratories can best integrate lessons learned, and respond to changing external constraints, through a flexible program management system, such as has been developed over the years with DOE program managers.

Overall, these factors constitute elements of an environment in which the DOE national labs can assume a leadership role in partnership with government program managers to define and manage substantial new initiatives that employ cutting edge science and technology. The white paper outlines policy recommendations for DHS, DOE, and the national laboratories with the objective of making the best possible use of laboratory resources in addressing homeland security challenges.

These implementation issues are related to the overall concerns about R&D risk management methodologies. The related elements, from probabilistic assessment of current scenarios, to decision making on defense and response alternatives, through the successful implementation and execution of R&D or procurement actions, are all included in the complete risk management cycle as illustrated in Figure 1 of this report. The formal methodologies for linking decisions to risk assessments, and for determination of successful execution strategies, are less developed than the traditional probabilistic risk assessments used in reliability and safety applications. However, the implementation end of the risk management cycle remains extremely important in the creation of new systems to reduce the likelihood and consequences of a major terrorist attack.

4. Concluding Observations

This research has examined the shortcomings of and potential improvements to the risk management processes used by the national laboratories and the Department of Homeland Security in fulfilling their homeland security missions. The risk assessment activities undertaken by DHS over the last several years have been important in assembling key national subject matter experts, intelligence analysts, and scientific data to inform current DHS decision makers regarding the critical technical aspects of WMD scenarios. The review in this research supports other evaluations in identifying the treatment of intelligent adversary decisions and the integration of analysis with program implementation as two areas in which the risk-based methodologies could be significantly improved. Two recent development programs at Sandia, and perhaps other outside approaches not reviewed in this research, offer new tools and methodologies to address these areas of concern. From the perspective of the DOE national laboratories, a number of other issues regarding successful program execution have also been identified and candidate recommendations offered. The overall risk management goal requires close attention to implementation issues in addition to identification of risks through probabilistic assessment techniques.

Distribution (PDF File):

1	MS 9004	J. M. Hruby, 8100
1	MS 9004	W. P. Ballard, 8100
1	MS 9004	P. K. Falcone, 8110
1	MS 9003	L. D. Brandt, 8110
1	MS 9003	J. Reinhardt, 8112
1	MS 9406	S. Gordon, 8114
1	MS 9406	T. West, 8114
1	MS 9159	P. Hough, 8964
1	MS 0757	G. Wyss, 6414
1	MS 9018	Central Technical Files, 8944
1	MS 0899	Technical Library, 4536
1	MS 0123	D. Chavez, 1011