

Statement for the Record  
Robert D. Jamison  
Under Secretary, National Protection and Programs Directorate  
Department of Homeland Security

Before the

Subcommittee on Transportation Security and Infrastructure Protection  
Homeland Security Committee  
United States House of Representatives

Tuesday, June 24, 2008

Thank you, Chairwoman Jackson-Lee, and distinguished Members of the Subcommittee. It is a pleasure to appear before you today to address the Department's implementation and execution of risk management practices. The Department of Homeland Security (DHS) is committed to the careful analysis of risk to inform a broad range of decisions. This commitment is demonstrated by the establishment of the Office of Risk Management and Analysis (RMA) within the National Protection and Programs Directorate (NPPD), the longstanding level of attention devoted to risk assessment and analysis within DHS components, and the collaboration in risk analysis across DHS components.

### **The Challenges**

Secretary Chertoff has reiterated the theme that no one entity—public or private—can effectively protect every single person at every moment in every place against every threat. Rather, the approach that the Department, indeed the Nation as a whole, must adopt is one of analyzing risk and using that information to devise the most cost-effective way of managing risk and improving security.

In the context of homeland security, estimating risk includes characterization of three key factors: threats, vulnerabilities, and consequences. Terrorist threats can change rapidly and adapt to new security measures, making the estimation of threat extremely challenging. Vulnerabilities are usually quantifiable through subject matter expert judgment and “red team” exercises that probe for weaknesses, but they vary widely for different scenarios or types of attack. The direct consequences of an attack are fairly straightforward to calculate, but it is very difficult to quantify indirect consequences, potential cascading effects, and the impact on the public psyche. Lastly, integrating terrorism risk assessments with other all-hazard risk assessments, such as natural disasters, is difficult. For these reasons, and many others, risk management in homeland security remains a complex and arduous undertaking.

Given these complexities in conducting risk assessments, there are two priorities when designing an overarching risk architecture for the Department. These priorities are:

1. Allowing for the development of customized, component-level risk analyses by analysts who know the unique characteristics of their mission space and the decision needs of their leaders and
2. Creating risk analysis guidelines and standards that will allow the Department to aggregate risk information across the broad spectrum of the DHS mission space to inform strategic decision-making.

The key challenge for DHS and RMA moving forward is to develop approaches and guidance materials that are both flexible and robust enough to accommodate these two priorities.

### **DHS' Risk Management Vision**

The Department's approach to risk-informed decision making has matured considerably over the past five years. It will continue to evolve as our understanding grows and as new analytic approaches are developed to deal with the complexities and uncertainties inherent in many of the risks for which DHS holds responsibility. Despite the progress already made, there is clearly much that remains to be done. The Department continues to focus on improving DHS risk assessment methodologies, advancing decision support tools, and identifying risk-related information gaps. For example:

- The Transportation Security Administration (TSA) has identified critical vulnerabilities within certain transportation modes, such as unattended railcars carrying Toxic Inhalation Hazards, and analyzes the mitigation of these vulnerabilities through the use of detailed metrics reports.
- The Office of Infrastructure Protection (IP) continuously tracks National Infrastructure Protection Plan (NIPP) implementation activities across all sectors. This allows IP to monitor the progress of establishing sector-specific risk management processes.
- The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts an annual risk assessment called the Strategic Homeland Infrastructure Risk Assessment (SHIRA) that spans across all Critical Infrastructure/Key Resource (CIKR) sectors.
- RMA has instituted a risk governance structure within the Department.
- The Federal Emergency Management Agency (FEMA) is modernizing flood maps to help communities improve their level of security from a natural disaster through smart building and setting of construction standards to create safer housing.
- The Office of Health Affairs is relying on risk assessments conducted by the Science and Technology Directorate to guide all of our bio-defense countermeasure strategies – both medical and nonmedical – and to inform our policies.

In all of these examples, DHS and its components are improving the Department's ability to develop information about risks and use this information to inform decisions. To advance these efforts, and to leverage the expertise, the Department must continue to further the integration efforts. Based on this key challenge, RMA, in collaboration with the Department's components,

has developed a vision to support the Department's efforts to advance its risk management capabilities. The vision is twofold:

1. Establish and institutionalize an integrated risk management framework. This framework will consist of the doctrine, principles, processes, guidance, and information flows that will enable risk-informed and cost-effective decision making within components and at the DHS headquarters level. A properly executed risk management framework effectively serves as a force multiplier, as it enables better alignment of security priorities and resources to needs.
2. Conduct strategic, integrated risk analysis. We must be informed, at the strategic level, by an integrated departmental risk assessment. The integrated risk assessment should leverage the various risk analyses being conducted within and outside the Department.

An integrated risk management framework will help better ensure that these efforts are harmonized and work from the same principles and understanding. Strategic, cross-component analysis will leverage the advances DHS' components have made with regard to risk management while incorporating those advances into DHS' larger planning and resource allocation processes.

### **Current Risk Management Practices**

The Department is tasked with fulfilling missions that range from finding persons lost at sea to detecting renegade nuclear weapons. Without a clear understanding of the risks facing our society, decision-making could become less effective. Our resources could be spent to protect the Nation against risks that are less significant, while we simultaneously fail to protect the Nation against the risks that are more critical.

NPPD, through RMA, is continuing to build the foundation for sound risk management practices across the Department. To enable the sharing and integration of RMA and component risk-related efforts, RMA has implemented a risk governance process within the Department. Central to this risk governance process is the DHS Risk Steering Committee (RSC) that RMA established. The RSC is comprised of risk analysis leads from across the Department and meets on a monthly basis. This approach ensures that there is collaboration, information-sharing, and consensus-building across the Department as we identify guidelines and recommendations for risk management and analysis. Currently, there are three working groups within the RSC. The efforts of the RSC working groups will provide the foundation for the integrated risk management framework and for strategic, cross-component analysis.

- The Risk Assessment Process for Informed Decision-Making (RAPID) Working group – RAPID is a strategic-level, Department-wide process that will assess risk and inform strategic planning, programming, budgeting, and execution processes. The process is focused on developing techniques to evaluate the risk reduction impacts of relevant DHS programs.
- The Lexicon Working group – The lexicon is a comprehensive glossary of words and terms relevant to the practice of homeland security risk management that will be used to

ensure better understanding of risk management terminology throughout the homeland security organization.

- The Best Practices Working group – The product is an inventory of risk management lessons learned and recommended procedures and guidelines that will be used to guide the components to ensure that the Department’s risk methods are coherent, consistent, and technically sound.

The RSC has also been a very useful means for DHS components to coordinate their risk management efforts with each other. Examples of the programs that have RSC representation and participation include:

- IP’s NIPP Risk Management Framework and its work with Federal/State/Local/Tribal partners in setting and pursuing CIKR protection goals and the establishment of Risk Integration and Analysis programs;
- The United States Coast Guard’s (USCG) Maritime Security Risk Analysis Model (MSRAM), which allows USCG to develop and aggregate risk information at the port, sector, area, and national levels, and which supports numerous Coast Guard/DHS planning and resource allocation efforts at the strategic, operational, and tactical levels;
- The Office of Science and Technology’s risk model, which analyzes the risk-reduction potential of various research and development initiatives.
- The Federal Emergency Management Agency’s (FEMA) grant programs that utilize a risk-informed approach by considering both the risk profiles of specific jurisdictions and the quality of the business cases that the grant applicants develop to mitigate the risk.
- TSA’s agent-based risk simulation model, called the Risk Management Analysis Tool, which takes into account that terrorists are a dynamic and adaptive adversary and allows TSA to identify the risk reduction value of any single layer of security within the U.S. aviation system.

These component efforts demonstrate both the quality and diversity of risk management efforts within DHS. The goal of RMA is not to mandate that DHS components use a certain tool or analytical technique to conduct their specific risk analyses. Instead, RMA is serving as the bridge to connect these existing efforts together and is building products and collaboration forums to better ensure they are harmonized moving forward. The DHS integrated risk management framework will embrace a wide range of analytical tools and techniques. Most importantly, the framework will help ensure that all DHS risk analysis efforts are transparent, defensible, and documented. It will also help ensure that these analyses can be leveraged for strategic, cross-component analysis at the DHS headquarters level.

Lastly, the RSC is a primary formal mechanism for the internal sharing of DHS risk information. However, a number of key external communications mechanisms are also in place at DHS because a critical part of the Department’s risk management practices is how it communicates and works with its State, Local, and Tribal partners. For example, through the NIPP, DHS has established a framework that enables stakeholders from the private sector and public sector to coordinate on risk management issues. Government Coordinating Councils and Sector Coordinating Councils have been established across all CIKR sectors. Active information exchange occurs through the councils and through the Homeland Security Information Network.

As the integrated risk management framework is developed, it will be shared with Federal, State, Local, Tribal and Private Sector stakeholders through these and other mechanisms that RMA is currently assessing.

### **Advancing Risk Management at DHS**

While we have made significant progress in our efforts to build an integrated, effective, and harmonized architecture for risk management at the Department, we are still in the early stages of a long journey. As a Department, we are striving to implement an approach where major decisions about investments, budgets, grants, planning priorities, operational posture, and security priorities are risk informed. To do so, we are moving toward an integrated framework of risk-informed decision-making where:

1. Decisions are framed to include an understanding of the risks associated with them;
2. Risks are identified, analyzed, communicated and assessed, so as to ensure we fully understand the nature of the problems we are trying to manage;
3. Alternative strategies for risk management are developed and analyzed for costs and benefits;
4. Decisions amongst these strategies are made with the best understanding of how they impact the risk; and
5. Decisions are monitored and reviewed so as to understand how they mitigated the risk.

Such a risk management process for decision-making will be applied across DHS to address strategic, operational, and tactical risks. As we move forward, the Department, through RMA and the RSC, expects to make this process the center of an integrated risk management framework.

In addition, DHS will continue to build the foundational efforts necessary to execute the framework and strategic analyses. These efforts will include the development of a risk management training and education program for both risk analysts and senior leaders, investment in new technologies for risk data collection, improved department-wide access to resources for modeling and simulation, and the identification of useful risk management metrics.

### **Conclusion**

As noted in the 2007 *National Strategy for Homeland Security*, the assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risk. We at DHS recognize that risk management within the context of homeland security is an evolving field. We know that there are improvements that we can make in applying risk management and analysis to support our decision making. We rely on collaboration with experts inside and outside the government to learn how we can improve our abilities to understand, communicate about, and manage risk.

Managing risk depends on accepting uncertainty; managing risk does not mean eliminating it. At DHS our goal with regard to risk management is to continually improve our ability to

understand and recognize those risks, while developing the processes and methods that allow us to use that information to make better decisions. Those decisions govern how we invest our efforts in increasing preparedness, protection, and, ultimately, homeland security.

Thank you for holding this important hearing. I would be happy to respond to any questions you might have.