

**STATEMENT OF JOHN P. PACZKOWSKI
DIRECTOR, EMERGENCY MANAGEMENT AND SECURITY
THE PORT AUTHORITY OF NEW YORK & NEW JERSEY
AND
MEMBER OF THE BOARD OF DIRECTORS
SECURITY ANALYSIS AND RISK MANAGEMENT ASSOCIATION - SARMA**

**THE GOODYEAR EXPLOSION:
ENSURING OUR NATION IS SECURE BY DEVELOPING A RISK MANAGEMENT
FRAMEWORK FOR HOMELAND SECURITY**

**BEFORE
THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION**

**WASHINGTON, DC
JUNE 25, 2008**

Chairwoman Jackson-Lee, Ranking Member Lungren, and members of the Subcommittee, thank you for the opportunity to testify on ways the Federal Government can build on the efforts of the Department of Homeland Security (DHS) and others in applying risk management practices to better secure our Nation. I am John Paczkowski, Director for Emergency Management and Security at The Port Authority of New York & New Jersey and a member of the Board of Directors of the Security Analysis and Risk Management Association.

The assessment and management of risk enables and supports the full spectrum of our national security and homeland security efforts, including decisions about when, where, and how to invest limited human and financial resources. In the face of multiple and diverse threats and hazards, we must accept that security risk – a function of threats, vulnerabilities, and consequences – is a permanent condition, but one that can be better managed through the creation of a well-integrated national framework.

As an emergency management and security professional that has successfully applied risk management practices at an agency level and across multiple transportation sectors, I have experienced the value of using these tools to support homeland security decision-making first hand. This experience, as well as my leadership role with SARMA, has provided me with broad exposure to the range of national efforts undertaken in the wake of the 9/11 terror attacks. I will be speaking with you from both perspectives today.

THE PORT AUTHORITY EXPERIENCE

The Port Authority is a bi-state public agency responsible for operating some of the New York / New Jersey region's most significant critical infrastructure. We manage all of the areas major commercial airports (Newark Liberty, John F. Kennedy, LaGuardia, Stewart, and Teterboro); its largest complex of marine cargo terminals (Port Newark and Elizabeth, Howland Hook, and Brooklyn Piers); and its network of interstate tunnels and bridges (the Lincoln and Holland Tunnels; the George Washington, Bayonne, and Goethals Bridges; and the Outerbridge Crossing). The agency also operates the Port Authority Bus Terminal, a major transit hub near the heart of Times Square and the largest facility of its kind in the world. Our PATH rail transit system is a vital trans-Hudson commuter link and was the target of a serious terror plot foiled by the FBI not long after the London and Madrid metro bombings.

The World Trade Center was our flagship facility and headquarters for over 30 years. We still own that site today and are responsible for its redevelopment. Among the nearly 3,000 lives that perished on 9/11, our agency lost 84 of its corporate staff, to include 37 Port Authority Police Officers. Having been twice the victim of significant acts of terrorism and endured numerous potential threats that thankfully never materialized, and as the owner and operator of vital transportation infrastructure that remain lucrative terror targets, no other organization is more acutely aware of the importance of homeland security than the Port Authority.

Following the 9/11 attacks, the Port Authority conducted a comprehensive series of security audits at all of its facilities. Performed by expert consultants, the results were staggering. Over 20 individual reports, 1,100 recommendations, and a potential cost, by staff's estimate, of just over \$1 Billion to implement. Moreover, there was no sense of priority among the recommendations. Management's reactions were predictable, and not unlike those of the Congress for the Nation at large: 1) Do we really need to do all of the things recommended?; 2) Assuming we do, if we can't pay for it all, what is most important to address first?; 3) How do we know what types of solutions will return the greatest security benefit given what we have to invest?; and finally, 4) How will we be able to measure the performance of those investments after they have been implemented?

Believing these to be the fundamental questions that would ultimately drive homeland investment going forward, we reached out for assistance to pursue our own security risk management program. Beginning in 2002, we partnered with DOJ, and later DHS, to develop and implement a risk assessment methodology to guide security planning and priorities for our initial five-year, \$500 million security investment program. The methodology permitted the agency to examine an array of potential security threats, assess the criticality of its assets, estimate the potential consequences of successful attacks, and make cross-sector comparisons of risk. Under a DHS technical assistance program, it has since been applied to 36 other transportation agencies across the country.

Following completion of our first assessment in 2002, we have subsequently repeated the process on a two-year cycle, updating security priorities, plans, and budgets in two successive iterations. In so doing, we have moved the agency from conducting individual

risk assessments to implementing an ongoing program of security risk management. As each risk assessment is conducted, the results are compared against the prior one and the change in relative risk is calculated. This comparison shows not only the improvement in the agency's risk profile as the result of new investment but also any changes arising from adjustments to our infrastructure portfolio or the overall threat picture. In this way, we can measure the "buy-down" in risk as a metric for security program performance.

In addition to measuring risk reduction performance, we have worked with DHS consultants to implement a cost-benefit analysis component to the methodology that facilitates comparisons of competing high-cost security alternatives. This tool permits us to evaluate which security improvements or, more importantly, which sets of improvements will provide greatest risk reduction "value" for the money invested and risk reduction potential to be achieved. We recently used this tool with great success in evaluating complex, high-cost alternatives for securing our PATH rail transit system, and will be applying it to the development of our long-range security investment plan going forward. The next evolution of the Port Authority's risk management program will go beyond security risks and examine a range of additional man-made and natural threats in an agency-wide, cross-sector, "all hazards" assessment.

To my knowledge, no other organization at the State and local level has advanced security risk management practice to the degree that we have at the Port Authority. Unfortunately, as successful as we have been, our risk assessment results are unique to our own agency and not compatible with other similar efforts on a regional, State or national level, and are therefore of limited value to DHS when assessing overall homeland security risk. Nonetheless, our success proves that new approaches to security risk management do work, and this fact should reinforce efforts by DHS, the Administration, and the Congress to advance risk management as a fundamental element of national homeland security policy.

Before the Administration and the Congress consider what to do next, it is important to note that risk assessment approaches are now being applied within a range of industry sectors, at different levels of government, by different agencies, using different methods, and with different objectives. As a new field, this is to be expected and to some degree necessary. However, we are now at an important crossroads and, in the view of the Security Analysis and Risk Management Association (SARMA), stronger and more unified Federal leadership on this issue is urgently needed to lead and coordinate the numerous duplicative and conflicting efforts in DHS and across the federal government.

THE SARMA PERSPECTIVE

SARMA is an all-volunteer, non-profit, professional association serving those responsible for analyzing and managing security risks to individuals, structures, systems, operations, and information. SARMA was founded in April 2006 by career security analysis and risk management professionals dedicated to fostering more effective public/private partnerships to advance consistent, risk-based approaches that provide decision-makers with measurable results for intelligently reducing security risks. The span of SARMA interest includes terrorism, intelligence collection, cyber crime, and

natural hazards. SARMA fosters an open collaborative and non-partisan environment to promote the further development, standardization, and professionalization of the security analysis and risk management discipline for the benefit of the American public, the nation's security, and the security profession in general.

SARMA's mission is to elevate the practice of security analysis and risk management to a mature, standardized, and consistent discipline among a growing cadre of formally trained and certified professionals, all working together to make the nation more secure and resilient. SARMA provides a vital link between the Government, the private sector, academia, and individual practitioners. Without this link, homegrown risk methods and theories tend to proliferate, making it even more difficult to coordinate protective efforts between all levels of government or with the private sector.

Over the years, significant resources have been expended by Federal departments and the private sector to implement security risk management processes and methods. However, despite the considerable sums spent to effect improvement, security risk management efforts remained largely unchanged until the terrorist attacks of September 11, 2001. The focus on homeland security that emerged after 9/11 resulted in considerable numbers of new analysts and consumers of security risk information, and also produced significant new funding for security risk management efforts. Nonetheless progress to advance a well-integrated national framework still lags.

DHS, other Federal agencies, academia, and the private sector have used newly available homeland security funding to develop and implement a wide array of new security risk methodologies, which are not necessarily coordinated or compatible in their approach. In addition, various homeland security directives and plans either provide conflicting guidance or remain silent on the security risk assessment methods to be used by Federal agencies, State and local government, and the private sector. As a result, almost seven years after 9/11, the Nation has yet to achieve a consistent and well-integrated risk management framework providing decision-makers at all levels with the ability to intelligently manage homeland security risk.

In SARMA's view, this is largely the result of the following factors:

Security risk management is an immature discipline that has developed independently and unevenly across the Federal Government and private industry.

DHS correctly seized on the applicability of security risk management to its mandate of protecting the homeland, but it has not taken steps to ensure the structure, processes, and cadre of qualified risk analysts are in place as necessary to effectively serve the mission. Accordingly, there is still no formal system or framework to standardize technical and professional development or to otherwise build the professional infrastructure required.

There is no national system of governance to guide risk practitioners and ensure collaboration and interoperability in development of risk management approaches.

Absent interagency coordination, an advisory board, and/or a recognized standard-setting body, there is no way to synchronize divergent methods, arbitrate disputes, or resolve crosscutting issues. As a result, risk practitioners often develop new methods rather than

adopt or adapt an existing approach. Because the underlying methods currently in use are not based on commonly recognized or compatible standards, the resulting data is often less than useful to others who must then collect similar data using another methodology.

There is no comprehensive, documented body of knowledge on the current state of the discipline from which to implement new security risk management efforts.

There are no common references that practitioners can consult when considering how to best meet their security risk analysis needs. Without such a body of knowledge, there is no way to determine where adequate methods already exist, decide where to focus additional research and development, or ensure existing efforts are not duplicative and wasteful. Moreover, without this collection of knowledge, it will be difficult to train the next generation of security risk analysts and managers in a consistent manner.

The lack of a common professional language for security risk analysis and risk management divides practitioners and makes collaboration difficult.

This “language deficit” serves as a significant impediment to a cooperative approach on security risk analysis and management between the Federal Government, State and local governments, and the private sector. While attempts to set standards within individual Federal departments and agencies have been made, conflict with similar efforts elsewhere only exacerbates the problem. Without a common language for use by practitioners, future progress will remain frustratingly slow.

There is currently no capability to train or certify the knowledge and technical skill of security risk management professionals and bring new entrants into the field.

Given the huge investments being made in homeland security, coupled with the central role of risk management, it would seem logical that training and certification of risk practitioners should be a national requirement. Unfortunately, there is no recognized approach to risk management training in Federal, State, and local government agencies, or in the private sector. Absent this, it is difficult to imagine that risk management will ever be done with the degree of reliability and compatibility that decision-makers require.

SARMA RECOMMENDATIONS

There are a few practical steps that can be taken within existing authorities, and the support of the Congress, to remedy the current situation and more fully realize the vision of more effectively managing security risks to the American homeland. Accordingly, SARMA recommends that the Administration:

Issue a joint National Security Presidential Directive (NSPD) and Homeland Security Presidential Directive (HSPD) to create a “National Security Risk Management Program.”

The joint NSPD/HSPD should establish a national program for security risk management, complete with funding for a system of governance over all Federal efforts to implement supporting risk management policies, programs and practices across the interagency community. Such a program would accelerate progress, reduce duplication of effort, and eliminate organizational conflicts and other barriers to implementation.

Require Federal departments and agencies to create a Chief Security Risk Officer (CSRO) appropriately positioned and empowered to synchronize, coordinate, and monitor all security risk management efforts within their organizations.

The Chief Risk Officer (CRO) concept has been in widespread use by the private sector for decades. Implementing such a position within key Federal departments and agencies would elevate the importance of security risk management and end debates over who creates necessary policies and procedures and leads security risk management initiatives at the department and/or agency-level. Though we believe that the initial focus of this position should be on coordination of security risk activities, the ultimate goal should be a convergence of all risk management activities within a consolidated CRO portfolio.

Establish a DHS CSRO and harmonize homeland security risk management policies and programs to ensure consistency, and as needed, compatibility and integration, not only within DHS but with State and local governments, and the private sector.

In addition to reconciling and ensuring coordination among all homeland security risk management policies and programs across the Department, the DHS CSRO should identify appropriate DHS agencies and offices to serve as homeland security risk management advocates to state and local governments and the private sector. This would extend the benefits of a common risk management framework to industry and all levels of government as part of a truly integrated and “national” effort.

Create a security risk management governance structure to span the interagency community and bring standardization and rigor to the assessment of security risks, while increasing overall confidence in the process and the decisions that result.

To this end, two essential elements of this structure are recommended:

A Chief Security Risk Officer (CSRO) Council. The CSRO Council would be officially recognized as the authoritative body for Federal security risk management strategy, policy, and standards. The CSRO Council should include security risk management officials from all agencies with significant homeland security and national security responsibilities. In addition, the CSRO Council would:

- Oversee the implementation of the joint HSPD/NSPD for a National Security Risk Management Program;
- Coordinate and set direction for national security risk management efforts; and ...
- Analyze and broker resolution of disagreements between Federal departments and agencies over security risk management issues.

An Interagency Security Risk Management Staff. This interagency staff function would serve as a security risk management Center-of-Excellence, providing program development support, technical expertise, and training to Federal, State, and local governments, as well as the private sector. The staff would address the shortage of qualified risk methodologists and trainers by centralizing that expertise and making it available to support practitioners in achieving the national goal of a mature, unified, and broadly-accepted approach to security risk management. The staff would:

- Provide technical assistance in carrying out security risk assessments and implementing security risk management programs;
- Provide security risk management training, establish minimum training and certification standards, and produce associated training materials; and...
- Maintain public/private partnerships to support the use of risk management in the implementation of national security and homeland security policies and strategies.

CONCLUSION

Homeland security efforts since the terrorist attacks of September 11, 2001 have highlighted the difficulty of protecting an almost infinite number of targets with finite human and financial resources. The use of security risk management is the approach correctly chosen by our Nation's leadership to address this enormous challenge. In response, considerable work is underway. Yet, in order to ensure the effectiveness of these efforts, the development and implementation of a well-integrated national framework for security risk management is needed.

The refinement and application of a more uniform and coordinated approach to analyzing security risks will greatly enhance our Nation's ability to understand and manage the multitude of threats we face, now and well into the future. That will then lead to improved decision-making and more efficient prioritization of resources by not only Congress and the White House, but by the thousands of State and local government and private sector leaders that make up the fabric of our national homeland security effort.

The creation of a national system of governance and standards for security risk management is beyond the mission and authorities of any one agency. The development of security risk management, as both a process and a profession, is a national priority that cannot be achieved by DHS acting alone. A well-integrated national security risk management framework will require a broad-based partnership with State and local government, private sector industry, academia, and related professional associations. Even with visionary leadership and direction it will not be easy, as the Government Accountability Office and others have noted. Yet such a framework is necessary if we are to protect the people, infrastructure, and economic prosperity of the United States.

SARMA encourages Congress, the White House, Federal departments and agencies, State and local governments, and the security profession to join forces and collaborate to achieve a national security risk management framework that will help provide the Nation with the protection and response capabilities it needs at a price it can afford. The members of the Security Analysis and Risk Management Association stand ready to assist Congress, the Administration, and DHS in whatever way we can to help advance this important initiative.