Statement For the Record

William G. Raisch
Director
The International Center for Enterprise Preparedness (InterCEP)
New York University

Testimony for the

U.S. House of Representatives Committee on Homeland Security
Subcommittee on Transportation Security and Infrastructure Protection
The Mumbai Attacks: A Wake Up Call for America's Private Sector

Wednesday, March 11, 2009
2:00 p.m. EDT Cannon House Office Building

The International Center for Enterprise Preparedness (InterCEP) of New York University
A Program of the Center for Catastrophe Preparedness & Response
113 University Place, 9th Floor, New York, New York 10003
Tel. 212-998-2000 Email: intercept@nyu.edu Web: www.nyu.edu/intercep

Chairwoman Jackson-Lee, Ranking Member Dent, and distinguished members of the Subcommittee, it is my sincere honor to again provide testimony to this committee.

I join you today as past private sector advisor to the federal 9-11 Commission and currently as Director of InterCEP, the International Center for Enterprise Preparedness at New York University. InterCEP is the world's first research center dedicated to private sector resilience.

In my capacity today, I am at best a channel for the many insights that are shared with the Center from hundreds of businesses and other organizations that participate in InterCEP forums and initiatives.

Our primary goal at InterCEP is simple. We work with key stakeholders to identify, understand and collaboratively solve real problems in the area of emergency preparedness, security, operational continuity and risk management.

I will now outline what we see as the current challenge of private sector preparedness (with a particular focus on the hospitality industry), the opportunity provided by the new Private Sector Preparedness Program (PS-Prep) and then address urgently needed actions in this arena for both government and business.

The Challenge

Preparedness can be generally seen as an effort to develop capabilities to prevent a hazard where possible (and feasible) and to mitigate the impacts of a hazard should it nonetheless occur including capabilities to respond and recover while maintaining continuity of core operations.

The significant law enforcement expertise assembled by this committee today can better comment on the specifics of appropriate prevention strategies for a Mumbai-style attack in the United States. Clearly such prevention strategies would likely involve effective public-private coordination in terms of advance warning and intelligence sharing, a heightened level of awareness among staff and customers alike as well as a level of physical security generally only applied to VIP appearances in our country.

I would like to focus my comments today on "all hazards" emergency preparedness which should be, but often is not, the general foundation upon which specific strategies to address any new or evolving threat is built. At the center of all hazards preparedness is preparing for the often common impacts of emergencies with common core capabilities. It involves developing capabilities for such activities as ongoing threat assessment and situation analysis, a clearly understood incident management structure, effective warning and crisis communications with employees and customers alike, basic resource management and logistics necessary to access needed supplies, targeted training and exercises as well as effective relationships and communications capability with public safety organizations. All hazards programs should be what we fall back on in the event of the unexpected.

Overall preparedness appears to vary greatly among businesses generally and key drivers appear to include the size of firm, experience with crisis and presence of regulatory requirements.[1]

- **Larger firms or facilities (with more overall staff and other resources) tend on the whole to be more prepared than smaller firms.**

- **Firms that have experienced a crisis or recurring threats tend to be more prepared than those that have not.**

    - For example, the well-established threat of room theft in hotels has resulted in the general addition of room safes and restrictions in some cases of who can enter guest room areas).

- **Firms that have regulatory requirements for overall preparedness (e.g., utilities and financial services firms) tend to be more prepared on a programmatic basis** than those that do not. Similarly, specific requirements for elements of preparedness (such as fire and life safety) are clearly prompted by regulation. Such codes play an important role in the hospitality industry.

- **Availability of financial resources and expertise is always a limiting factor.** Unfortunately, security and preparedness expenditures are generally considered by most firms to be "overhead" costs and these have been severely cut and likely will continue to be further eroded should economic conditions worsen.

    - In the hospitality industry this can be exacerbated by the franchise system, whereby major hotel corporations may manage properties but these are owned by their franchisees who may have to approve operating budgets. While issues such as life safety and food safety are considered must do regulatory requirements and are an accepted element of budgets, security is often considered optional in nature.

Even among the most prepared firms, research suggests that preparedness and security overall can be significantly improved. But to maintain even the current levels of preparedness will require sustained funding but the current economic environment is resulting in significant across-the-board cutbacks to the area of preparedness and security.

[1] While there is still no consensus-based measurement of preparedness for the private sector (pending the implementation of PS-Prep), we can draw on personal observations, anecdotal information and what might be considered indicators of preparedness elements such as surveys of expenditures on security or the presence of certain plans or programs. From these inputs, overall assertions can be made.

The Need

In large part, it can be argued that the current situation is due to a lack of a clear "what" to do, "how" to do it and a compelling "why" to do it. In line with our prior testimony to this Committee, several factors contribute to this situation primarily focused on these three considerations:

- **<u>What to do</u>: A set of clear criteria for what constitutes effective preparedness and security is needed.** The criteria for what good preparedness is can be difficult to ascertain. There are a diversity of strategies, technologies and approaches to preparedness and effective security. Most firms are not aware of any standards in this regard.
    - The criteria must optimally be derived from the private sector and based upon actual business experience to assure that it is applicable in the business environment.
    - Current successful industry practices must be acknowledged and built upon not displaced. As with a number of other industries, the hospitality industry has significant history internationally as well as domestically in the security and preparedness arena; this experience should be at the core of any effort.
- **<u>How to do it</u>: Implementation strategies including risk assessment methodologies, training and planning resources are necessary to apply the general criteria to specific business facilities/operations.** "How" preparedness criteria (if identified) should be applied to a particular operation may not be clear. Size, geographic location, type of industry, current intelligence, etc. all can inform the nature of preparedness actions to be undertaken. Likely a small motel along an interstate does not require the same approach as a large hotel property next to an iconic building in a major city. How should risks be identified and prioritized? What training is necessary? What resources are available to support planning and implementation?
    - A risk-based methodology that can identify and prioritize risks and inform prevention, preparedness, response and recovery activities is vital.
    - Appropriate training and other tools necessary to develop and implement preparedness programs on a company basis are needed.
    - Public-private partnerships in information sharing and intelligence with an emphasis on actionable information must be sought.
- **<u>Why to do it</u>: A compelling business case and the development of new incentives for preparedness with linkage to the common criteria is needed.** The business case for preparedness is not always evident. Preparedness requires investment of time and resources. Businesses invest in efforts that increase profitability. It is not apparent to most businesses that an investment in preparedness will either increase revenue or decrease expense. The probability of hazards and their potential impacts on a business are difficult to assess. The perception that "it's not going to happen to me" is widespread. Thus, unless there are clear

bottom-line reasons or regulatory requirements for preparedness and security, activity in this area tends to be minimal.

- An approach is needed that does not rely solely on the risk of terrorism at the primary motivator (which will likely be discounted by many) but rather looks to the common impacts of many different risks on an operation and focuses on common strategies of preparedness, response and recovery which can be established at a relatively lower cost than developing a number of individual risk specific programs.

- A serious and ongoing research effort must be developed that not only documents current anecdotal impacts of preparedness but also develops new approaches to more comprehensively clarify the economic benefits of preparedness to the corporation and wider society.

- The active engagement of key stakeholders in the development of new incentives must be promoted and maintained.

An Opportunity: The Private Sector Preparedness Program

The new Private Sector Preparedness Program (PS-Prep) championed by this Committee and reflected in Public Law 110-53 holds great promise in addressing a number of these needs. It is as you know, currently under development by DHS. Key elements of the program include the following.

- **The program is to be based on existing business preparedness standards by the private sector based upon its experiences overtime**, not by government.

- **The program will be risk-based**. All of the standards in this arena require as a starting point a risk assessment and thus would suggest activity appropriate to the risks identified for each operation and not a one-size-fits-all approach.

- **Core standards in the arena also incorporate cost-benefit analysis** as part of their processes. Thus, firms are encouraged to prepare reasonably and to the extent of available resources based upon true business value.

- **The program is poised to be link preparedness overtime with potential benefits and incentives.** InterCEP currently has five Working Groups involving approximately two hundred individuals providing input on linkage to potential incentives overtime in supply chain management, legal liability mitigation, rating agency acknowledgement, more rationalized business reporting on preparedness and insurance.

Nonetheless, the PS-Prep Program is only an element of a more comprehensive strategy needed to secure our businesses in general and the hospitality industry in particular. Additional elements are included below.

Critical Next Steps

There are several critical steps necessary to move forward preparedness within the private sector as a whole including the hospitality industry. Critical next steps must be taken by the Department of Homeland Security, Congress and businesses.

The U.S. Department of Homeland Security (DHS):

- **DHS must designate one or more core standards as soon as possible to move the PS-Prep certification program forward.** While promising, this program is far from complete and the designation of standards is a necessary precursor to further activity. The Department has discussed the program with the private sector widely through a diversity of forums. It has developed and vetted its target criteria for the choice of standards and announced them publicly in the Federal Register. It has held two highly interactive national meetings with the private sector on the program. Now is the time to move forward and designate the one or more standards required by the legislation.

- **DHS must continue to support the efforts of the designated accrediting body, ANAB, to assure that this program has a firm base in the historically proven private sector voluntary accreditation process.** ANAB has administered accreditation programs in such areas as quality management (ISO 9000) and environmental management (ISO 14000) for decades. It has established relationships with the business sector and a time-validated approach to conformity assessment of businesses.

- **DHS must support an outreach to the critical infrastructure sectors to engage them in the ongoing development and implementation of the PS-Prep Program.** These sectors are vital to a resilient society and they often have a well developed appreciation of the importance of resilience. This outreach must
    - Educate these sectors on the opportunity presented by certification program.
    - Clarify the program as an opportunity to identify and credit best practices already existent in each sector and not an effort to supplant existing and effective practices where they exist.

- **DHS must fund and work with appropriate stakeholders to support the mapping of existing industry specific practices in preparedness and security, especially those in the critical infrastructure sectors.** The common criteria of the new certification program offer a unique opportunity to identify and categorize good practice in these sectors.

    - Such a mapping could be used to assist in crediting these practices in the PS-Prep Program, so that those industries and companies with strong preparedness programs would be appropriately recognized.

- Furthermore, and perhaps more importantly, this mapping could create an opportunity to cross-walk practices across industries allowing for cross-pollination of approaches and strategies. Such an effort could create a "rosetta stone of preparedness" which could establish a more robust body of good practices for all organizations. InterCEP is actively looking to engage with key industries in this regard.

- Given the importance of the hospitality industry and its history to date, this industry could be one of the initial targets for collaboration on a mapping of existing practices.

- DHS should coordinate this effort but consider that the outreach might best be undertaken in conjunction with non-governmental parties to minimize potential concerns about creeping regulation.

- **DHS must support and fund the development and delivery of training to assist in implementing the common criteria of the PS-Prep program.** Key professional associations should be considered for this effort including the American Society for Industrial Security (ASIS), Disaster Recovery Institute International (DRII), the National Fire Protection Association (NFPA) and the Risk Insurance & Management Society (RIMS).

- **DHS must support and fund the development and delivery of appropriate tools to enable implementation including risk assessment methodologies and online resources.** Risk assessment tools such as RAMCAP Plus (developed by ASME-ITI) should be considered. Online resources such as the DHS Ready.gov site, the Open for Business ® planning tool offered by the Institute for Business & Home Safety (IBHS) and the Red Cross Ready Program from the American Red Cross should be considered.

- **DHS must support and fund a first wave of company certifications under the PS-Prep Program.** Participants should include high profile, opinion leading companies with significant supply chains as well as their suppliers including small businesses.

  - This will provide a proof of concept and an opportunity to test the program out on a small scale before being rolled out on a wider basis.
  - Lessons learned can be captured and used to inform the wider effort, including lessons for both large and small businesses.
  - Leading corporations can both become familiar with the certification program (on a pilot basis) as well as provide high profile leadership.
  - By including corporations with significant supply chains, these initial undertakings could set the foundation for supply chain focused resiliency initiatives underscore a clear economic rationale for preparedness among small businesses. Such efforts could involve larger corporations working with a targeted group of their critical suppliers. In various InterCEP forums, several leading corporations have already indicated their interest in potentially mentoring their key suppliers in preparedness.
  - This first wave initiative should be funded by DHS and potentially utilize the DHS grant mechanism.

- **DHS must support and fund a long term seminal research project to begin to measure the economic value of preparedness overtime. This project could ultimately provide the most compelling rationale for widespread investment by the private sector in resilience.** There is no data on the impact of programmatic preparedness because prior to the inception of PS-Prep there has been (a) no commonly accepted definition of what constitutes effective preparedness and (b) no method to measure if these preparedness criteria were in place. Lacking these fundamental elements (a definition and a measure), there has no ability to see if prepared companies fare better after emergencies occur versus those companies that are not prepared. This lack of data has kept preparedness as a commonsense strategy but one that lacked any financial rationale that informed the real value of investment in preparedness. Hence, corporate efforts have tended to be notional and other actors such as insurance and rating companies have failed to strongly acknowledge and reward preparedness. They have lacked any real actuarial data on this vital area. With the PS-Prep Program in place, a long term project can now be undertaken to identify different outcomes overtime based upon whether or not a firm is "prepared" as indicated by its PS-Prep status. InterCEP seeks to be instrumental in this undertaking.

Congress:

- **Congress must continue its active oversight of key programs and initiatives.** Congress' wide perspective on this arena is critical to a comprehensive and sustainable strategy for private sector and overall society resilience.

- **Congress must fund DHS, FBI and other stakeholders as appropriate to enable the above initiatives** including the accrediting body required by the legislation, the mapping of existing industry practices to the common criteria of the designated standards, training and tools necessary to implement preparedness, the first wave of company certifications under the PS-Prep Program and the long term research initiative.

Businesses:

- **Businesses must look to the PS-Prep program for voluntary guidance and, as a first step, undertake an informal internal assessment of their operations based on the criteria of the program.** Core to this will be an initial risk assessment to inform what preparedness measures are appropriate. Further application of the PS-Prep program should be considered if it presents additional business value.

- **Additionally, businesses should evaluate the use of the PS-Prep Program in assuring supply chain resilience, especially for suppliers of mission critical services to core business operations.** Firms with high priority needs and regulatory requirements for continuity such as the utility and financial services industries should especially evaluate this opportunity to assess the resilience of their critical suppliers.

- **Businesses must actively partner with government in information sharing and other public-private partnerships.** Information gained from these partnerships can inform risk assessment as well as other preparedness, response and recovery activities. Federal programs include DHS Sector Coordinating Councils, DHS Information Sharing & Analysis Centers (ISAC's), DHS Protective Security Coordinator Division, FBI InfraGard, U.S. State Department Overseas Security Advisory Council (OSAC). State and city programs such as Chicago First, NYPD Shield, New York City Office of Emergency Management CorpNet/PALMS and the wide diversity of others should be considered. Private not-for-profit organizations such as Business Executives for National Security (BENS) should also be considered.

- **Businesses should consider participation in first wave of company certifications under the new Private Sector Preparedness Program.**

- **Businesses must promote and participate in an industry-by-industry effort to map and recognize existing preparedness and security practices utilizing the criteria of the PS-Prep certification program as the organizing theme.**

Finally, all parties must work to assure that resilience is designed into our nation's infrastructure projects from the beginning (not added after a crisis). We must <u>prepare</u> as we <u>repair</u> and expand our infrastructure. The private sector and federal, state and local governments must take constructive action to assure this.

- Our goal must be to create a more resilient nation as well as a better supported one.

- Adding resilience considerations at the design stage can generally be done at minimal costs. Yet, resilience can pay big dividends in reducing the cost of future disruptions that are inevitable due to both natural and manmade hazards.

- Risk assessments should be a standard step the advance planning for all infrastructure projects. Such risk assessments could lead to designing in appropriate mitigation and prevention measures for identified hazards as well as measures which could facilitate response and recovery in any crisis, large or small.

- Existing strategies should be utilized to advance resilience including the both programmatic standards such as those under the PS-Prep program as well as risk assessment tools such as RAMCAP Plus.

- Infrastructure projects should consider local, state, regional and federal preparedness planning.

- In addition to protecting our people, a more resilient infrastructure will make for a more competitive America in the global marketplace.

Our Center stands ready to assist wherever appropriate and collaborate with all key stakeholders in the achievement of these critical initiatives.

Respectfully submitted:

William G. Raisch
Director
International Center for Enterprise Preparedness (InterCEP)
New York University
113 University Place, 9th Floor
New York, New York 10003
212-998-2000
intercept@nyu.edu
www.nyu.edu/intercep