Reprinted with Permission from DomesticPreparedness.com

The New Preparedness Challenge: Transitioning Resilience from Theory to Reality

by DENNIS R. SCHRADER

Wed, February 10, 2010

Working professionals in the Domestic Preparedness community are already familiar with the once vague term “resilience” – but will soon learn more. A lot more – primarily because resilience seems to be an increasingly important component of the Obama administration’s national security strategy, particularly in the area of homeland security. The White House has, in fact, already created a high-level group to explore the concept in much greater detail. Coincidentally, last month, Philip Palin outlined an argument – in *Homeland Security Affairs* – that the U.S. “Grand Strategy” for Homeland Security should be focused on resilience.

Much earlier than that, though – i.e., in 2004 – Dr. Steven Flynn was an early activist in developing the theory that the resilience of the nation’s infrastructure should be a key security strategy. He and others raised the consciousness of homeland security and emergency management professionals.

The fact is that great endeavors require not just vision, but also human and financial capital – as well as a compelling drive over many years to turn the vision into reality. If resilience is going to transition from theory to reality, therefore, the nation’s engineering and financial communities will have to work together in a meaningful long-term effort. Engineers in particular will have to become more integrated into homeland security and to learn much more about emergency management structures and processes.

The Department of Homeland Security’s Science and Technology Directorate (DHS S&T) has already completed some important preliminary work on the importance of resilience, and recently sponsored an interesting study (*An Operational Framework for Resilience*) that was released in August 2009 by the Homeland Security Studies and Analysis Institute. That study examined not only the “hard infrastructure” but also the “soft operational components” of resilience – including topics such as individual preparedness that contribute to business continuity.

Moreover, in a July 2009 paper presented at Columbia University, Mitchell Erickson of the S&T directorate examined the issue of engineer and scientist roles in resilience efforts – and also pointed out that resilience is and should be a capital cost that has to be justified on a project by project basis.

Meanwhile, the National Infrastructure Advisory Council (NIAC) developed and published a practical report (in September 2009) that examined resilience as “necessary for government and business to create a comprehensive risk management strategy.” In that report, the NIAC concluded that current market forces may be inadequate to achieve resilience for high-consequence/low-probability events because the business case for investments by the private sector cannot be justified. The report also argued for market-based incentives to encourage resilience.

ASCE’s Role; the NIAC Report; and Market-Based Incentives

Engineers will have to become more sophisticated as risk managers during project development. This idea has been advocated by the American Society of Civil Engineers (ASCE) in two of its own studies: “Guiding Principles for National Infrastructure”; and “Vision 2025.”

The need for and use of market-based incentives are, in fact, the crux of the issue. The challenge is that infrastructure resilience is still not a well defined, and well understood, area of practice and expertise. Resilience is, though, a design outcome that, as observed in the NIAC report, “complements infrastructure protection” and therefore requires a thorough analysis of interdependencies between infrastructures.

The private sector has begun recognizing that infrastructure resilience is more than just a matter of security, but is also the foundation of the nation’s economic prosperity. That recognition led to creation of The Infrastructure Security Partnership (TISP), which was formed by eleven professional and technical associations, and federal agencies, not long after the 9/11 terrorist attacks and since then has been a strong advocate of practical engineering-oriented resilience strategies in both the public and private sectors.

Complementing the TISP efforts, ASCE has been producing an “infrastructure report card” for several years. Resilience was added as a factor in the most recent (2009) Report Card. The bottom line of all of these initiatives can be described in just a few words: Achieving Resilience will be a journey – not a destination. For that reason:

- It will require a collaborative effort that brings engineers and business owners/operators as full partners into the Homeland Security and Emergency Management “Community of Professionals.”
- It also will require the appropriate government agencies to re-examine the overall Preparedness Process, with special focus on such important and interrelated topics as Mitigation, Protection, Recovery, and Resilience – which should collectively be viewed as a systems engineering challenge rather than as separate functional elements.
- Most important of all, perhaps, it will require private-sector governance boards and financial institutions to develop, and effectively use, metrics that value resilience as a major priority.

If resilience is going to transition from theory to reality, the nation's engineering and financial communities will have to work together in a meaningful long-term effort; engineers in particular will have to learn much more about emergency management structures and processes