



Reprinted with Permission DomPrep Journal September 15, 2010

Resilience: Developing Professionalism, Clarifying the Incentives

by DENNIS R. SCHRADER

Wed, September 15, 2010

The U.S. Department of Homeland Security's Quadrennial Homeland Security Review (QHSR) of February 2010 and the more recent DHS Bottoms-Up Review (BUR) of July 2010 have led to greater awareness of the importance of resilience as a fundamental element of the nation's disaster readiness requirements. The key to improving resilience capabilities, it could be argued, will be establishing more and stronger links between government public-safety agencies and the private-sector professional continuity and engineering communities.

The QHSR focused special emphasis on the need to strengthen and mature the nation's Homeland Security Enterprise to support five principal mission areas, including resilience. The most important factor for success in achieving that goal will be the ongoing development of national security professionals who understand the entire national enterprise – i.e., federal, state, local, non-governmental, and private-sector environments and resources.

Within the next decade, it now seems probable, U.S. national-security professionals will be much more comfortable with the lexicon of resilience and therefore more capable of focusing on the tangible implementation of a more effective resilience strategy. It is currently not clear from the BUR what specifically will or should be done differently from the methods and practices of the past decade. It may simply be, of course, that focusing on resilience as a strategy could create different implementation approaches. However, it is becoming increasingly clear that there are three primary components of resilience: (a) *Community Preparedness* – not only the general population's understanding of the principal threats but also the commitment of the American people to be much better prepared; (b) *Operational Resilience* – i.e., the ability to continue operations both during and after an incident; and (c) *Systems Design* – as demonstrated by a continuing effort to build resilience into the critical infrastructure and networks during the development stage.

Although there have been some minor successes with its resilience attempts during the past decade, the federal government has limited ability to create effective and enduring change for each of these elements through centralized Washington programs. Each of the "components" mentioned above requires an understanding of the basic incentives associated with them in order to develop workable and effective policies and programs to encourage resilience.

Core Concerns, Advance Planning, Standards, and Networks

One of the core concerns for most state and local governments, as well as private-sector businesses, is that security and disaster preparedness (SDP) will have to be included in budget planning as another "cost of doing business." Because SDP therefore becomes a cost center, rather than a revenue center, achieving low-cost, sustainable solutions to SDP is the primary goal that will have to be pursued. One effective way to meet that goal would be by using low-cost, lightweight networks that are necessarily linked through national policy, but not directly controlled by the federal government.

For example, the most important keys to operational resilience are advance planning and business continuity. DHS recently adopted the National Fire Protection Association (NFPA) 1600 as one of its voluntary Private Sector Preparedness Standards (PS-Prep); that action could and should encourage greater resilience in the private sector.

The Disaster Recovery Institute International is an organization that has credentialed over 8,000 continuity professionals throughout the world. DRI International is, of course, now cross-referenced in NFPA 1600 as a source.

The private sector will ultimately be motivated to keep businesses operational simply to maintain profitability – which, of course, is the "prime mover" in the world's industrialized nations. By linking with organizations

such as DRI International, governments can use the business-continuity network to link the private sector to national resilience policies – and that in itself would be a considerably different way of thinking about such issues than was the custom in the past.

Another key business-continuity strategy is to focus greater attention on supply-chain networks. Because of the Year 2000 "end of the millennium" problems, many businesses began looking more seriously at their supply-chain vulnerabilities. That effort has evolved into a routine business protocol for many if not yet all of the nation's larger private-sector companies.

Probably the most relevant question a public safety or national security professional must now ask is, "How much do I know about organizations such as DRI International?" The same question is valid for businesses and organizations involved in community preparedness and system design. Businesses are concerned about community preparedness in order to keep their own workforces intact. The engineering and construction community that supports the existing environment, for example, obviously wants to ensure that businesses are able to continue in operation both during and after a major incident.

SDP resources are already limited, though, and probably will be even more constrained in the future. For that reason alone, it is obvious that the more the U.S. public safety community learns to leverage private networks, the more resilient the nation will become.

The most important factor for success will be the ongoing development of national security professionals who understand the entire national enterprise - i.e., federal, state, local, non-governmental, and private-sector environments and resources