

Summit tackles tough issues

Emergency response organizations meet to discuss key issues for state and local preparedness

BY AMY C. HUGHES

The nation's principal state and local emergency responder associations met for the second time this year to continue an in-depth dialogue on all-hazards emergency preparedness and homeland security. The National Emergency Preparedness and Response Partnership Summit II, hosted by the National Emergency Management Association, was held in Washington, D.C. on June 11-12.

Homeland security advisors from 12 states joined representatives from state and local law enforcement, public works, emergency management, fire, public health, public safety communications, emergency medical services, and National Guard associations to engage in open discussions about the issues facing the nation's emergency preparedness and response system.

Three issues dominated the conversation: the national plans and strategies released by the Department of Homeland Security, communications interoperability, and critical infrastructure protection.

The national strategies

Within the past year, the Department of Homeland Security and the administration have released three strategies that have a profound effect on the emergency responder community: *The National Strategy for Homeland Security* (July 2002), *The National Strategy for Physical Protection of Critical Infrastructures and Key Assets*



(Feb. 2003), and *The National Strategy to Secure Cyberspace* (Feb. 2003).

The summit participants discussed these national strategies – including the ongoing federal initiatives and the grant programs that support them – and what they do for the emergency responder community, what they do not do, and what implications they have for state and local governments.

The discussions revealed several areas in which state and local officials see opportunities to strengthen the existing framework:

- While the strategies outline the common goals and objectives in achieving homeland security, there is no guarantee that these goals will be accomplished. The strategies note the need for more widespread intelligence information-sharing. More can be done to ensure that state and local governments and private sector officials have access to timely, relevant

threat intelligence on which they can allocate resources and make the best decisions.

- All three documents set forth the priorities but more guidance is needed on how to implement them. The Homeland Security Advisory System establishes a warning system for the nation, but specific recommendations are needed to guide public and private sector entities on what actions they should take as the levels are upgraded. Many state and local governments are working together with key industry sectors to develop guidelines and recommendations on actions to support changes in threat levels.
- The national strategies do provide funding and establish accountability for achieving the primary goals, but more flexibility in the use of funds is needed. State and local leaders are working with the Department of

Homeland Security and congressional leaders to promote flexibility to allow state and local governments to properly match funds with their priorities. At the summit, participants provided feedback to U.S. Sen. Susan Collins' staff on the Homeland Security Grant Enhancement Act of 2003, which proposes to streamline the homeland security grant process.

As a follow-up to the National Strategy on Homeland Security, the White House released Homeland Security Presidential Directive 5 in late February. In the document, the administration directed the Department of Homeland Security to develop a National Response Plan and a National Incident Management System, which are intended to integrate separate federal response plans and establish a single, comprehensive approach to domestic incident management. A first draft of the NRP and NIMS was distributed to major stakeholder organizations and federal agencies in late May for review and comment.

State and local stakeholder organizations have noted the need for greater opportunities such as this to provide feedback to the department to ensure that emergency responders' perspectives are considered when legislation, plans and programs are developed. Enhanced communication and collaboration among all levels of government is the key to turning the strategies into realities.

The human factor

Summit participants also discussed the lack of communications interoperability. According to a recent publication by the National Task Force on Interoperability, the lack of coordination and cooperation among agencies and departments is one of five key reasons why public safety agencies don't communicate. The NTFI report, *Why Can't We Talk*, is available at <http://www.agileprogram.org/ntfi/>. Federal, state and local agencies are only just beginning to recognize the "human element" of public safety communications.

In a multi-jurisdictional response to a disaster, emergency responders will inherently operate under the communication protocols and operational culture of the unit to which they are assigned. Simply

buying new equipment or standardizing police radio codes, or "10-codes," won't fix the problem.

According to Deputy Chief Charles Werner of the Charlottesville, Virginia Fire Department, human interaction is 70 percent of the problem when it comes to achieving communications interoperability. "All of the money and technology combined cannot overcome the human barriers that still exist between public safety agencies," he said. "More can be done to achieve interoperability through strong interagency relationships based on trust, respect and concern for the well being of one another."

To truly achieve a seamless network of public safety communications, jurisdictions must also have "organizational" interoperability. Multiple agencies that are not accustomed to working together must now plan and exercise together to prepare for short- and long-term disaster responses. A culture of coordination and collaboration must be established to ensure that the perspectives of law enforcement, emergency services and public safety support agencies are considered.

"Ideally, state and local leaders must define the new standard of interoperability (communications and operations) and accept nothing less," Werner said.

Summit attendees also participated in a discussion on critical infrastructure protection facilitated by the National Infrastructure Institute's Center for Infrastructure Expertise. Like communications interoperability, there is a human factor to consider when prioritizing the importance of the nation's assets. Currently there are no standardized national tools or models for state and local governments to use when identifying critical infrastructure. Among the various methods states are using to determine the impact of the loss of assets, most leave out the psychological effects of attacks on certain targets.

The USA Patriot Act of 2001 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." However, an attack on a soft target such as a shopping mall,

although not considered a critical asset, may cause an economic and psychological ripple effect that cannot be accurately forecast with numbers and formulas.


"One only has to think back to the Washington, D.C. area sniper attacks last year to appreciate the potential economic and 'fear factor' impact that terrorists can cause," said David O'Keefe, director of the NI2 Center.

At the summit, O'Keefe announced the launch of the Critical Infrastructure Clearinghouse, located at <http://www.ni2ciel.org>. The clearinghouse will serve as a one-stop shop for government, private sector and academic information on critical infrastructure and key asset protection.

Taking action

At the end of the summit, participants agreed that a more formal partnership should be established to facilitate the exchange of information and dialogue, and where appropriate, to articulate to the Department of Homeland Security positions on critical issues. This fall, participants will discuss the idea in greater detail at a meeting of NEMA's Homeland Security Committee. The national coordination group includes the major emergency responder associations and representatives from the main state and local government associations."

After the summit, several organizations drafted a letter to Homeland Security Secretary Tom Ridge offering the expertise of state and local officials to further refine the draft National Response Plan and the National Incident Management System. They encouraged the department to allow state and local experts to assist early in the development process of future national plans and strategies for homeland security.

In addition, the representatives agreed to support federal initiatives to advance mutual aid and communications interoperability, to maintain base funding for public health and safety across all disciplines, and to more regularly communicate their positions on federal legislation, plans and strategies. 

— Amy Hughes is a policy analyst for the National Emergency Management Association, an affiliate of The Council of State Governments.