

## Collaborative Technologies for Public Safety

Events like 9-11, Oklahoma City, the Madrid train bombings, the December 2004 Tsunami and Hurricane Katrina in 2005 have taught valuable lessons to those of us in the military, law enforcement and public safety communities. We continue to see weaknesses and vulnerabilities. We have seen time and again that in multi-jurisdictional incidents command and control problems become exacerbated by communications, accessibility and technology issues that are further confounded by the natural fog of confusion surrounding a disaster. A strong step in helping responders see thru this fog will be accomplished by NIMS (National Incident Management System). Developed by the Department of Homeland Security and issued in March 2004, the NIMS will enable responders at all jurisdictional levels and across all disciplines to work together more effectively and efficiently. Beginning in FY 2006, federal funding for state, local and tribal preparedness grants is tied to compliance with the NIMS. NIMS strengthens the concepts of an Incident Command System (ICS). ICS was developed to provide Federal, state, and local governments, as well as private and not-for-profit entities, with a consistent framework for the preparation for, response to, and recovery from any incident or event, regardless of the size, nature, duration, location, scope, or complexity. ICS systems go back to the early 1980's and many jurisdictions have implemented many kinds of ICS systems.

A key component that we've seen time and again is the ability of first responders, rescue, recovery and disaster aid personnel to communicate and collaborate critical information accurately and in real-time. There are numerous barriers to collaborative practices amongst different agencies. Silos of information exist but no connections exist between these silos. In the 21<sup>st</sup> century, the technology exists to bridge these silos; it is now the cultures that must be bridged.

Technology gives us the ability to "virtualize" our response processes. Our traditional EOC's (emergency operations center) have an inherent weakness as we all saw in New York after Sept 11th, and on the Gulf Coast after Katrina. The EOC and it's backup locations can be easily impacted by an event. Key personnel can be unable to get to primary and secondary locations. So we increasingly turn to technology to create "virtual" EOCs (VEOC). A VEOC can have a nearly infinite reach. We can evacuate operations to the comfort of a Holiday Inn miles away or tie in key people who are on vacation or otherwise in distant and remote locations. Collaborative technologies provide responding organizations with tremendous power and reach. Technology platforms from a variety of suppliers present powerful tools for the responders and all require training and training integration.

But using these tools requires a new mindset and a new training paradigm. The good news is that these tools don't require significant changes to our operations. We still collect the same information, distribute to the same people and take the

same actions. We can now do this faster, more effectively and more accurately. These tools allow unprecedented interactions between groups and provide real time information sharing.

In the training business we say "train like you fight". A collaborative response plan for a VEOC or virtual EOC is no different. Here is a short listing of simple rules for implementing and training to VEOC collaborative technologies within a jurisdiction.

- 1) NIMS exists for a reason. Use it. Connecting different agencies, language and cultural issues create stumbling blocks. If your agency has not yet adopted "clear text" or "clear language" rules...do so. Reports, broadcasts, situation reports and the like must be in clear, concise English.
- 2) Technology is a tool. Never be enthralled by the latest technology. Don't let the IT (information technology) guys make your operational decisions. The tools that will work for you are the ones that fit your jurisdiction's SOPs (standard operating procedures) and response protocols. The IT guys need to support your mission. The simpler the technology the easier it is to access it, use it and support it. Look at solutions that require no client-side (desktop PC software) and work entirely via an internet web browser.
- 3) Go wide and deep. Think about your CEMP (comprehensive emergency management plan) or other protocols you have. List ALL of the agencies involved. Include the civilian groups and NGOs such as the American Red Cross, Salvation Army and United Way. Include ALL the players in your training and exercises. Groups that work together and train together before an incident occurs, execute more effectively during the incident.
- 4) Apply training to reality. We retain learning depending on how we obtain the learning. Research studies have shown that when learning we retain about 5% of what we get in lecture and 75% of what we learn by practice (or learning by doing). But we retain 90% of what we learn when there is an immediate application for what we learned. So when implementing these collaborative technologies, having people prepared to start using them a month (or two or three) from now will result in low retention and high re-training requirements. Have a program in place where people will go immediately from training to usage. One tactic is to require the course evaluation form to be completed the day after training using the tools that were trained. If no formal program for usage is in place, create a collaborative team working group so people can meet virtually and provide feedback from their locations and jurisdictions.
- 5) Keep it real. All too often we see that training exercises are based on extreme scenarios. Many times I've participated in exercises involving

a terrorist/WMD/radiological attack in downtown \_\_\_\_\_ (insert city of your choice). Now these things are very important, and must be practiced. BUT, we all know what types of events are prone to occur in our areas. There will most likely be another hurricane in south Florida before a terrorist attack. Southern California is well aware of earthquake possibilities. Developing appropriate multi-hazard exercises will always pay off in the long run. We all saw that Hurricane Katrina created multiple hazards within one incident ranging from snipers, to toxic chemical spills to search-and-rescue and more. We didn't need al-Qaeda to create terror in Louisiana and Mississippi. Temper this concept by remembering that "anything can happen at anytime".

- 6) Define how, what and why you collaborate. It may be enough to access real-time situation reports. On the other hand you may require the ability to share reports, files, maps, images and even video conference. Look at how your jurisdiction does business today and how you want to do business tomorrow.
- 7) Budget and then budget some more. There is a misconception that collaborative technologies for emergency management are an expensive proposition. It does not have to be. Web based discussion boards can be implemented for pennies per user. Full scale solutions with document sharing and audio/video can be hundreds of thousands. Start with what makes sense for your jurisdiction, something that is supported by your budget and don't overlook grants.
- 8) Define the needs of participants. The community of people in the classroom may be very diverse depending on your jurisdiction. Fire/Rescue will have different immediate concerns than then Police Department, and different again will be the Health Department. Jurisdiction based trainers will have an entirely different point of reference. Prior to training, attendees must be oriented to understand the eventual goals of using collaborative technologies. In addition, jurisdiction management needs a plan and organization for both implementation and usage that is clearly communicated to attendees. Just saying that you will "virtualize the EOC" may sound great and very high-tech but participants will need details related to their jobs, functions and roles.
- 9) Keep it fun. These collaborative tools are fun to use. Make sure that makes it into the training programs. It is a given that we learn more when we have fun doing so. For example, create virtual communities to share things outside of emergency management; start discussion groups about local restaurants, cultural events or sporting events. These are also things that may someday need a response of some kind.
- 10) Use it, use it, use it. If these technologies are not used, then they will be lost. Find reasons to utilize the tools. Make up excuses to use it.

- Instead of having that weekly staff meeting, make it an online virtual meeting.
- 11) Play nicely with others. Invite support and partner agencies to participate in your training process and in your exercises. They are important and should be treated as such. For example, county government may ensure all local PD's participate. And invite the Red Cross and Salvation Army liaisons as well.
  - 12) Learners are not sheep. People will not blindly follow this path without a good, solid foundation. Learners can be told the operational reasons and implications of what these tools will do. Planning how your agencies' SOPs, processes and procedures will interact with these tools will be a critical point of integration for learners. Plan it, plot it and prepare it. Make sure that training answers the questions that will come about the operational interfaces.
  - 13) Trainers are Trainers are Trainers. We see all too often that trainers for some of the specialized software applications come from academic, educational or software backgrounds. Always make sure that the trainers being provided to your agency come from real-world applications in the field as well as expertise in the tools. To be effective in training your organization, the trainers must be able to relate to, understand and guide learners based on personal experience.
  - 14) Train to a ConOps. Base the training on your organizations concept of operations (ConOps). Use your existing structures and workflows and use the tool to support, not change, your processes. Once the tool is learned, you can "tweak" or modify your procedures. If you do not have developed ConOps or SOPs (standard operating procedures), these technologies will not develop them for you.

We have found that applying these rules when implementing the new technologies paves the road to success. Consistency in planning, consistency in training and the mantra "Semper Gumby" (always be flexible) are keys to any emergency management and response plan.

-----30-----

**About Paul Seldes**

*Paul Seldes is an experienced public safety professional with 25 years experience in developing complex training programs for a variety of municipal, state and federal agencies. Mr. Seldes worked at Ground Zero in New York after the September 11<sup>th</sup> 2001 attacks and hurricanes in Florida and Mississippi. As a senior partner at Celeriti, he oversees development and delivery of training programs for a wide variety of organizations. He currently resides in Florida. He is a member of the International Association of Emergency Managers (IAEM) and the Florida Emergency Preparedness Association (FEPA). Mr. Seldes can be contacted via email at [paulseldes@celeriti.com](mailto:paulseldes@celeriti.com). Information about Celeriti, LLC can be found at <http://www.celeriti.com>.*