

IP-based mass notification technology makes big impact in 2010



By Guy Miasnik

Applying the capabilities and power of the network to alert people to threats and emergencies -- and to plan a course of action in response to them -- made a real difference in protecting people and enhancing national security efforts last year.

The recent shootings at Fort Bliss and the University of Texas–Austin campus have clearly demonstrated that network-centric emergency mass notification systems have worked as designed, helped to protect the individuals in those communities and enabled them respond to their respective crises.

As the emergency mass notification technology provider at Fort Bliss and at major U.S. military commands, as well as the technology of choice at many government entities, including the U.S. Coast Guard (USCG), AtHoc sees firsthand how government agencies use network-centric mass notification as part of their emergency preparedness strategies. This innovative technology has been applied to situations ranging from helping the Coast Guard respond to the Gulf oil spill, to delivering alerting capabilities to the U.S. military stationed at home and deployed abroad.

IP network-based alerting provides a range of communications paths so notifications can be sent to multiple and redundant channels and devices from a desktop computer, to the individual cell phone, to a social networking site, all in order to reach people anytime and anywhere in case of an emergency. Leveraging an existing IP network is the most cost-effective, most efficient model for alert communication and management for situations large or small.

At Fort Bliss, the mass notification system enabled alerts to be communicated instantaneously over the computer network, as well as by phone. The system worked successfully, without error, accord-

ing to press reports.

At the height of the Deepwater Horizon Gulf oil spill disaster, the Coast Guard's Alert and Warning System 2.0 (AWS 2.0) emergency notification system was used for critical external communications, such as waterway closures due to the oil spill and to communicate about ports that were open. In addition, the mass notification solution was employed for communicating internal mission-critical information, such as personnel recalls, to assist with response to the oil spill and notifying Coast Guard staff to report to the appropriate Coast Guard command center.



Examples of communications used during the response to the spill include a Coast Guard notification sent to internal and external users that Port Fouchon was open, correcting misinformation about that port being closed. An internal notification was sent to USCG Sector Honolulu requesting additional personnel for the spill operation. The Coast Guard's Sector Mobile in Alabama used AWS 2.0 to postpone a search-and-rescue exercise that was scheduled for the Gulf near the spill.

The Coast Guard embraced network-centric emergency communications with its AWS 2.0 centralized server-based system that replaced a previously used cumbersome notification process which depended on a string of actions at the unit level, often without central coordination from the Coast Guard headquarters and regional offices.

AWS 2.0 improves the Coast Guard's ability to account for the reception of messages and alerts by taking advantage of the way IP-based services -- such as e-mail and text messaging -- enable immediate replies. Using AWS 2.0, the Coast Guard can rapidly and reliably transmit targeted alerts in bulk to maritime partners and stakeholders. It also allows the Coast Guard to receive responses from alert recipients to support the Coast Guard's multiple missions.

AWS 2.0 provides a single enterprise solution that is capable of sending alerts concerning safety, security and environ-

mental protection events to Coast Guard personnel and maritime industry members; can automate unit personnel recall and continuity of operations; and can manage personnel accountability in times of crisis. Since its deployment, AWS 2.0 has been used extensively to manage Coast Guard and federal responses to crises, including the earthquakes in American Samoa and Haiti.

The U.S. Air Force used network-centric alerting during the aftermath of the earthquake in Haiti, where the Air Force was able to alert and account for 300,000 people to ensure that the military knew their welfare and whereabouts, including their families. The benefits of the Air Force's network-centric emergency notification system includes the ability to send hundreds of thousands of alerts across virtually every channel in minutes, capture responses for personnel accountability and enable first responder coordination.

As can be seen by real-world emergencies faced by government agencies in 2010, the accurate and timely delivery of information via network-centric emergency notification enables emergency preparedness, prompt reaction and effective countermeasures. ■

Guy Miasnik is CEO and president of AtHoc, a provider of network-centric notification solutions for the U.S. federal government. He can be reached at: gmiask@athoc.com