

# PUBLIC SAFETY REPORT

COMMUNICATIONS SOLUTIONS FOR PUBLIC SAFETY

## CONTENTS

EMERGENCY ALERT SYSTEMS 61 4.9 GHZ FOR BACKHAUL 66  
INTEROPERABILITY WITH PROJECT 25 70

# 12 LESSONS for Emergency Alerting

**Use technology and planning to help protect your most mission-critical assets.**

By Guy Miasnik

In any emergency response, the primary objective is to get help to those who need it as quickly as possible. But many obstacles lie in the way of a rapid response during an emergency. Confusion, misinformation, and rapidly changing circumstances all underscore the need for fast dissemination of information. Effective emergency alerting can remove those obstacles and promote a safe and timely response.

Emergency alerting has experienced a significant transformation during the past decade. Although sirens, public address systems, and the Emergency Broadcast System were already in place to assist with mass warning, the past 10 years has witnessed the birth of personalized, targeted alerting. We've seen the rise of automated telephony alerts, e-mail alerts, text messaging, and most recently, the introduction of network-centric alerting systems.

Currently, a single network-based emergency notification system can simultaneously send alerts to all forms of alerting channels with the click of a mouse. Individuals, large groups, or the public can be alerted with detailed information about an emergency situation. The alerts provide relevant information while also allowing for acknowledgement and feedback, helping ensure personnel accountability by determining who has received an alert and whether they need help.

The U.S. Department of Defense (DoD) has driven much of this transformation. In its efforts to prepare for



The DoD pioneered an alerting system from which critical infrastructure could benefit.

any eventuality, the department has actively pioneered the use of technology to ensure information dissemination and personnel accountability in times of emergency. It has deployed emergency alert systems that can reach hundreds of thousands of personnel in minutes, sending information to all forms of communications devices, including computers, phones, mobile devices, sirens, and public address systems.

The lessons learned and the best practices the DoD derived from building such large-scale alert systems for highly dispersed populations are relevant to emergency managers responsible for protecting the facilities, businesses, and infrastructure that serve as the backbone of the United States and Canada.

Today, critical infrastructure is grossly unprepared for the challenges that lie ahead. More often than not, the lack of preparation stems from a fundamental lack of understanding of what's at risk when an emergency occurs. Recent events — such as Hurricane Katrina and the shootings at Virginia Tech — have opened eyes to some of the possibilities.

Many of our nation's most important assets are outside the federal government's protection. It's estimated that 90 percent of the critical infrastructure is in the hands of the private sector and state and local governments. Water, energy, transportation, schools, ports, and financial systems

must all be protected for the country to continue to function effectively.

The DoD has invested significant time, effort, and resources in creating a list of best practices, many of which can be implemented as part of an emergency alerting strategy. The best practices have been used so extensively in the military that some of the services have created regulations and instructions around the recommendations and requirements.

### Alerting Actions

Facilities can learn from the valuable lessons gained by the DoD's efforts to deploy emergency notification systems for facility security and personnel protection. These best practices include:

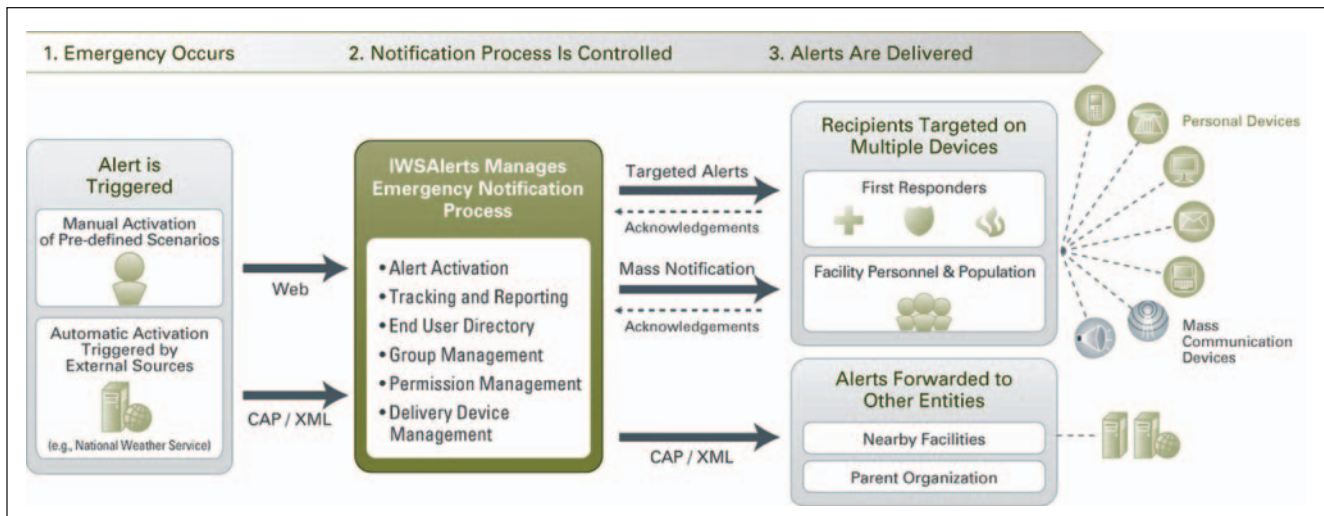
**1. Network-based alerts for rapid and assured mass notifications to individuals and shared kiosk computers.** Transform existing IP network infrastructure into an instantaneous, pervasive, and cost-efficient mass warning system, reaching any network-connected computer via intrusive popup alerts. Leverage the network's capability for assured, prompt delivery to every recipient's workstation with acknowledgement of receipt. Use existing kiosk computers, lab workstations, and other shared computers as a network-based computerized warning station, providing both audio alerts and instruction for action such as an evacuation map for people in the vicinity.

**2. Phone notification for limited targeted personnel and data notification to the masses.** Use phone alerts for a small subset of the population such as first responders and leadership. Phone alerts take longer to deliver, require more communications resources, and may get congested in times of emergency if used for mass communications. To reach a larger audience, use digital messaging — desktop alerts, text messaging, and short message service (SMS) — to communicate quickly to reach both onsite and off-site personnel. Note that e-mail is not regarded as an effective means of emergency communications.

**3. Redundant multichannel alerting reaching personnel wherever they are.** Use all forms of mobile and land-based communications devices — including laptops, desktops, shared computers (kiosks), cell phones, pagers or PDAs — for alerting. Messages are sent as desktop popup alerts, text messages, or audio alerts depending on the device. Apart from notifying people wherever they are, this approach provides redundancy of communications channels, which is highly important for emergency notification systems.

**4. Single activation of all notification systems.** By using a network-centric, unified alerting management system, the DoD can alert all network-connected devices, as well as other traditional forms of alerting, such as public address, sirens, and telephony, all managed and triggered from a single, centralized system. This reduces response time, assures consistency of the message, creates redundancy between delivery media, and reduces training and management resources required.

**5. Alerting personnel with special needs.** The DoD actively supports alerting to people with disabilities and special needs in compliance with the U.S. Rehabilitation Act, Americans with Disabilities Act, and related presidential directives.



**6. Reliable recipient contact information.** The unspoken challenge of collecting and updating personal contact information for all personnel is a major challenge for any emergency management team. Only select enterprise-class systems can provide the tools required to efficiently handle this problem. Such tools include synchronization with organizational user directories, sometimes with multiple directories in parallel; the ability to let emergency operators supplement such information; the capability to let users self update their information; and flexible distribution list management.

**7. Establish standard operating procedures for emergency notifications.** Emergency notifications should be an inherent part of any emergency response plan. Incident scenarios should be planned in advance and include who to notify, the message content, delivery devices, and the expected responses. It's also important to define in advance who is allowed to approve and/or activate the emergency notification procedure.

**8. Distributed management and activation.** In large organizations, emergencies may happen in a specific facility or apply only to a certain department. To shorten response time and improve command and control, the DoD allows local security officers with restricted and secure

access to launch alerts to personnel under their jurisdiction — whether a specific facility or department.

**9. Web-based secure access.** The DoD is moving toward Web-based systems that can be activated from anywhere so operations center personnel can access a network-connected Web browser. This provides a safeguard should an operations center become disabled or inaccessible during an emergency. It also enables activation of alerts by field operators directly from the location of the event, using wireless network connectivity. DoD alerting systems must have the ability to incorporate authentication and security permission tools. Only people with proper permission can log into the system and trigger alerts.

**10. Automatic monitoring of emergency information sources.** Network-centric alerting solutions monitor information sources, such as the National Weather Service, U.S. Geological Survey (USGS), etc., for the ability to automatically trigger alerts to emergency managers when certain conditions are met, improving situational awareness.

**11. Forwarding capability.** DoD alerting systems give managers the ability to forward alerts to other facilities in the region or to community emergency services. This type of “cascaded notification” allows an alert to flow from a point of origin to other first response and impacted organiza-

tions and supports interoperability among entities.

**12. Emergency warning system sustainability.** Alerting systems must always be available. This requires planning for all eventualities that could disable the system. To address this challenge, the DoD deploys a backup system, preferably in a different location, to assure continuity of operations even if the main system has been disabled. It also creates server redundancy and fail-over support.

Use these best practices as appropriate within your organization. They can offer guidance about what to look for in emergency alerting offerings, and they can also spur ideas about how to plan in advance for a wide range of emergency scenarios.

The DoD is tasked with protecting our troops — an important job — and DoD officials have created the most comprehensive alerting networks in the world. Why reinvent the wheel? You can benefit from their work. By implementing emergency alerting as part of your emergency response plans, you can directly impact your agency's ability to respond effectively to any type of situation. ■

Guy Miasnik is the president and CEO of AtHoc. The company's technology is widely used across the DoD, protecting more than 800,000 military personnel. Contact him at gmiasnik@athoc.com.