

What is the National Incident Management System (NIMS), Part 2



By [Leo Wrobel](#), [Sharon Wrobel](#)

Date: Oct 3, 2008

[Return to the article](#)

Leo A. Wrobel and Sharon M. Wrobel conclude this series by examining the National Incident Management System (NIMS) standards for communication and the various types of commands within the Incident Command System (ICS).

[Part 1](#) of this series discussed the fact that any emergency could be recoverable through the use of fundamental standards, strategies, and communications. In developing the [National Incident Management System](#) (NIMS), the U.S. government hoped to ensure minimal loss of life and infrastructure during any major event. In the conclusion of this series, we delve deeper into the NIMS standards for communications and technologies as well as the different types of commands within the [Incident Command System](#) (ICS).

Communications and Information Management

We've all heard the old axiom that real estate success is about three things: location, location, location. Arguably disaster recovery is all about communications, communications, communications. The cornerstone of any recovery plan is the ability to garner an accurate situation analysis about the event and to respond with specific instructions. The most critical communications are likely to occur in the first two hours.

Communications of all types should flow through people who are properly identified, certified, and predefined as holding the responsibility, and who meet certain security standards. Whether this person is an Incident Commander, a First Responder, or the Public Information Officer, strict guidelines and protocols should be followed before relaying critical information at the time of an event, planned or unplanned. [Part 1](#) of this series described how the Public Information Officer (PIO) works within the guidelines of the Joint Information System (JIS). This standard is intended to keep all emergency information consistent throughout all responding agencies.

Communications such as indications and warnings can be disseminated in many ways, including incident notifications, public warning systems, or via the media (Amber alerts and the like). Communication can also take the form of incident notification, status, and situation reports. In a nutshell, the various entities involved in an event need to know what's going on, in order to make informed decisions and to carry out the appropriate actions. This information needs to be *factual* as well as timely. In times of disaster, the rumor mill can run rampant.

Where and how communications occur are just as important as who gets the information and when it's received. Often, communications may need to be sent to an emergency operations center (EOC), incident command post, and/or multiagency coordination entities (MCEs), so that these organizations can direct the response intelligently. In addition, how MCEs communicate with one another (depending on the specific circumstance) has a huge bearing on the effectiveness of the response.

Within the Incident Command System, three different commands are set up for specific types of emergencies:

- A **single incident command** handles things like a local telephone cable cut or a break in a water main. Usually, only local employees are necessary to handle the situation.
- If an oil tanker or a truck carrying volatile chemical agents turns over and spills into a river, a **unified command** might have to be set up, because more than one agency would have to get involved at the scene.
- Unlike the other two types of commands, an **area command** has no predetermined location and is not immediately recognizable. An area command would be set up in a public health disaster such as a chemical or biological threat, or if the event spanned several days. If a disaster covers several counties or states and/or involves multiple agencies, it becomes a unified area command to allow for proper representation at the area command. Unlike the incident command post, an area command has no operational responsibilities per se. Specific responsibilities directly associated with the response are carried out under the umbrella of the other

two commands. Obviously, it's important that processes are in place to ensure the consistent exchange of communication, data, and resources at all times throughout the various command

Continuity of communications is conveyed by means of using common terminology and through the development of standards. These standards include ensuring that both voice and data transfer with communications equipment is not only interoperable, but compatible. As in everything, planning and preparation are required ahead of time. Luckily NIMS provides standards for the installation, upkeep, and use of emergency systems. By incorporating different forms of communications in advance, such as wireless or radio, the issue of command and control after a disaster can be resolved before the occurrence of an event; and regardless of what kinds of communications mediums survive.

Supporting Technologies

Through the use of various technological systems such as voice and data communication systems, information management systems, and data display systems, essential technology is delivered and processed to support incident management activities within the NIMS framework. Processes are researched, tested repeatedly, developed and refined to ensure that everything goes smoothly when the systems are needed. Moreover, as new technologies come to light, they're evaluated for future implementation.

Consider today's outbound notification systems, which are designed to get the word out after a catastrophic event. In past [articles](#), we've repeatedly [stressed](#) the need for 4C (command, control, communications, computers, and intelligence) for a military level of control in any disaster response. It's no coincidence that these concepts originated during the Cold War. At that time, responders had 20 minutes to decide whether a hot bloom in Siberia was a gas well or something really terrible. Set in that context, a false positive and a false negative were equally unacceptable. Today, given the war on terror and other factors, responders have caught up with things that only the military needed in days past.

The challenge of deploying an effective outbound notification system is a growing concern facing nearly every commercial business, school, community, and municipality today. All organizations need the capability to detect a crisis situation, develop an effective communication method, disseminate information, and track response in a timely manner. A successful solution that proactively delivers relevant, prompt alert communications in emergency situations saves time and resources, ensures productivity, and, most importantly, saves lives.

Many such systems are available today (run a web search to see for yourself). All of these systems can help keep you from reinventing the wheel, and many are downright affordable for the control and pace of mind that they can bring to your organization. An ideal notification system enables an organization to respond appropriately to all sorts of emergencies: tornado, hurricane, or tsunami warnings; terrorism events; Amber alerts; campus alerts; hazardous chemical spills; medical pandemics; and so on with communications to all stakeholders, anytime, anywhere.

Almost all of these products have features that are desirable in setting up and maintaining 4C, and they're not all based on telephone systems. For example, one product offers a means of delivering content-triggered alerts and web-based applications for emergency notification. This same product monitors [National Weather Service](#) feeds for all 50 states, Puerto Rico, and the Caribbean, utilizing [National Oceanic and Atmospheric Administration](#) and [Department of Commerce](#) information. This information is then dipped against an alerting database developed with the specific customer to determine precisely how the information is to be disseminated, under what conditions, and/or what the triggering event is. For example, a listing of callers who tried to call 911 center but couldn't get through due to a cut cable or flood could actually be *text messaged* to another working device, such as a wireless phone or VoIP phone. Such interesting and useful technologies were available in the past only to the military, but are increasingly appearing in the commercial and public sectors.

Other interesting technologies:

- The [NIMS Incident Resource Inventory System](#) (NIMS-IRIS) is a support technology that transmits data to laboratories using standardized analysis processes. This inventory software-based system allows for accessing critical resources for a given event. It's simple, easy to use, and tracks everything from equipment to people. (No license fees are involved, which is a big plus.)
- The [NIMS Compliance Assistance Support Tool](#) (NIMSCAST) is a self-assessment tool that follows an event from preparation to final recovery.

Summary

While we'd love to expound further on the advantages of a NIMS framework and the standardization and advantages it provides contingency planners and first responders, we're out of space. We hope that you have enjoyed these articles.

Remember that even the smallest changes you make in your response plans can add up to a total improvement. You can provide a greater measure of security and certainty in a disaster and further protect the lives dependent on the solutions you provide. Best of luck and happy planning!

Leo A. Wrobel has more than 30 years of experience with a host of firms engaged in banking, manufacturing, telecommunications services, and government. An active author and technical futurist, he has published 10 books and more than 400 trade articles on a wide variety of technical subjects. Leo served 10 years as an elected mayor and city councilman (but says he is better now). A sought-after speaker, he has lectured throughout the United States and overseas and has appeared on several television news programs. Leo is presently CEO of Dallas-based TellAWCom Labs Inc. and b4Ci, Inc. Contact Leo at 214-888-1300 or email leo@b4ci.com.

Sharon M. (Ford) Wrobel served as corporate secretary and director of personnel for Premiere Network Services Inc. prior to joining b4Ci, Inc. in 2004. During that time, Sharon was instrumental in getting Premiere certified as the first CLEC to be certified in all 50 states, by aiding in filings and attending hearings. She also engaged in extensive research for Premiere, a function she continues with b4Ci as vice president of business development. Sharon was also president of the Ellis County Early Childhood PTA and the Ovilla Lions Club. She attended the University of Maryland and El Centro College in Dallas and received training as a registered nurse before joining Leo in business in the late 1990s. Sharon also served as a public official by accepting appointments to the local Planning and Zoning Commission and the Historical Commission.
