

What is the National Incident Management System (NIMS)?



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

Date: Sep 26, 2008

[Return to the article](#)

In this two-part series, Leo A. Wrobel and Sharon M. Wrobel discuss the implementation of the National Incident Management System (NIMS), which is designed to help communities throughout the U.S. to handle various emergency and disaster situations

Throughout our extensive research in disaster recovery planning, we've found that great number of government and non-governmental entities in the U.S. are being required to adopt national standard for handling various emergency and disaster situations. Most emergencies can be handled on a local level, but what about those that cross jurisdictions? For instance, how do the private sector, government, and non-governmental entities work in concert to handle an act of terrorism or a natural disaster? Most importantly, how do they communicate with each other?

What Is NIMS?

For any complicated profession, standards are a good thing. In fact, we've devoted many years to the subject of operating and security standards for disaster recovery. Other organizations, such as the [Disaster Recovery Institute](#), professionally certify standards in disaster recovery. Actual standards and practices for how all the aspects of recovery planning relate to one another have been elusive over the years, due in part to the newness of disaster recovery planning as a profession. Perhaps the [National Incident Management System](#) (NIMS) will help, at least for government agencies, which now are required to adhere to a NIMS-compliant framework in their recovery plans

NIMS came about for many reasons. The lessons learned fighting intense wildfires in California in the 1970s resulted in a fresh look at standards and procedures. Deaths, injuries, and property losses and resulted from miscommunications and management insufficiencies, rather than lack of resources or improper procedures. One problem that surfaced was that too many people were reporting to one supervisor. Other problems:

- Different emergency-response organizational structures
- Indistinct lines of authority
- Inaccurate incident information
- Vague or unspecified incident-response objectives
- Lack of proper training
- Inadequate or conflicting communications
- Deficient structure for coordinated planning between agencies
- Terminology differences between agencies

On February 28, 2003 President Bush issued [Homeland Security Presidential Directive-5](#) (HSPD-5), which directed the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS).

HSPD-5 required federal departments and agencies to make the adoption of NIMS by state and local organizations a condition for federal preparedness assistance (grants, contracts, and other activities) by fiscal year 2005. Obviously, some time has passed since HSPD-5 was enacted, but when it first came into being the directive specified that jurisdictions could comply in the short term by adopting the [Incident Command System](#) (ICS). Other aspects of NIMS required additional development and refinement to enable compliance at a future date. At the same time, the Secretary of Homeland Security established the [National Integration Center \(NIC\) Incident Management System Integration Division](#) to oversee and provide strategic direction for NIMS

To provide a national framework for handling all the aspects of a disaster or major incident, NIMS came up with five components that work together

- Command and management
- Preparedness
- Resource management
- Communications and information management
- Supporting technologies

We discuss the first three of these areas in the following sections. Part 2 of this series will discuss communications and technologies.

Command and Management

One part of the NIMS management structure is the Incident Command System. The ICS is used throughout the lifecycle of an incident, defining the operating characteristics, management components, and structure of incident management organizations.

The beauty of using ICS is that it has several built-in features that make managing any incident from acts of terrorism to hazardous material spills to a local city's planned emergency event a lot easier than in earlier times. The use of common terminology makes identifying facilities, members of a facility, and what takes place in that certain facility recognizable by the facility's name, which is less confusing for all involved. For instance, an *incident command post* would have an *incident commander*, and within that post specific identifiable activities would ensue. There can be only one incident commander for each incident, and he or she is just called *Commander*. The head of each section is called the *Chief* (see Figure 1).



Figure 1

The incident action plan (IAP) communicates the incident objectives for both operational and support activities. The plan addresses what is to be done, who is responsible for getting it done, and how communication will take place, as well as providing procedures and protocols for dealing with all aspects of the event. The IAP is developed for an operational period lasting 12 hours or longer. These plans depend on management to carry through a coordinated response, ensuring that everyone involved is going in the same direction toward the same goal.

Another part of the NIMS organization structure is the *multiagency coordination system*, containing a lot of the same components as the Incident Command System, but with the addition of *emergency operations centers* (EOCs). Established by emergency management agencies at the state and local levels, EOCs are the facilities that coordinate resources and information to support incident activities. Multiagency coordination systems may also include *multiagency coordination entities* where emergencies cross jurisdictions.

Public information systems are responsible for disseminating information to the public in a timely and accurate fashion during emergency events. In this system, the *Public Information Officer* (PIO) gives his or her recommendation to the incident command post. The PIO keeps control of the rumor mill, while alerting the public and the media of the facts regarding the emergency. This is not without procedures or protocols. The PIO works within the *Joint Information System* (JIS), which enables the PIO to disseminate the same information to all agencies. This support system is used by the decision-makers.

Preparedness

To be prepared for an emergency, before any incident happens you have to address the answers to a series of questions that will occur:

- What is the nature of the emergency?
- Which jurisdiction(s) is (are) responsible?
- Who is called into action and who stays back?
- What and where are the resources needed to respond to this emergency?
- Is it a short-term or a long-term recovery?
- How do you handle the emergency in the long term?

As part of NIMS, jurisdictions must develop several different types of *emergency operations plans* (EOPs) for responding to various emergencies. Then there are *procedures*, which provide all the essential information for responding to the emergency. *Preparedness plans* describe how to obtain resources through mutual aid agreements, which facility and equipment to use (depending on the event), and even what training will be utilized. After an event, planned or actual, is a need for a *corrective action plan*, which evaluates how objectives were met and the incorporates lessons learned into an updated procedure. *Recovery plans* explain the objectives for facilitating long-term recovery.

Resource Management

The tools used by incident commanders during an event are inventoried and made available by the various resource managers. Resources need to be categorized, activated, dispersed, and deactivated throughout the lifecycle of an incident. A request for resources comes from the incident Commander. If this request cannot be fulfilled through local channels, it must be submitted through the applicable emergency operations center or multiagency coordination entity, using standardized procedures that are already in place.

Summary

Without proper standards, strategies, and fundamental communications, the result of handling any emergency would be chaos. With the implementation of NIMS, the U.S. government intends to ensure minimal loss of life and infrastructure during a major event.

Part 2 of this series will delve into the NIMS standards for communications and technologies, as well as the different types of commands within the Incident Command System and its structure.

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.
