Taking **Command** of EMERGENCY RESPONSE

Semen Salivanchuk/Getty Images

A Primer on the National Incident Management and Incident Command Systems

BY KENNETH C. ECK

Emergency incidents that require the specialized planning and responding skills of industrial hygiene and OEHS professionals are occurring with greater frequency. It is incumbent upon professional first responders and planners to ensure that we can easily integrate ourselves into the response system. Two of the most important aspects of planning for and responding to wildland fires, hurricanes, hazardous materials incidents, confined space rescues, and other events are the Incident Command System (ICS) and the National Incident Management System (NIMS). Education and training in ICS and NIMS are required for all responders, including IH and OEHS professionals, regardless of the role they play within the incident response.

A BRIEF HISTORY OF ICS AND NIMS

In 1970, the Laguna Fire burned more than 175,000 acres of California forest. At the time, it was the third largest wildland fire in California history. After-incident reviews of the fire identified the following issues with the response:

- poor communication
- lack of an orderly, systematic planning process
- no prepared plan for the integration of agencies and resources into a common management structure and planning process
- "freelancing" by individuals without direction from a central command and without coordination with other first responders
- lack of common terminology
- lack of accountability, including unclear chain of command and supervision

Following the Laguna Fire, a group of response agencies, referred to as FIRESCOPE, gathered to evaluate these problems and develop a management system that would improve the response to similar incidents. These efforts led to the creation of the Incident Command System. Throughout the 1980s and 1990s, ICS became the most recognized and accepted management system for responding to emergency events within the emergency response community.

The need for a comprehensive National Incident Management System was identified following the terrorist attacks of Sept. 11, 2001. ICS became an integral part of NIMS, and the system was expanded to include local governments, industries, and businesses in addition to typical emergency response agencies.

INCIDENT COMMAND SYSTEM

ICS is a management system that provides a clear and concise framework for planning for, responding to, and controlling an emergency incident. ICS is designed so that it:

- meets the needs of a jurisdiction to cope with incidents of any kind or complexity (that is, it expands or contracts as needed)
- allows personnel from a wide variety of agencies to combine rapidly into a common management structure using common terminology
- provides logistical and administrative support to operational staff
- is cost effective by avoiding duplication of efforts and continuing overhead
- provides a unified, centrally authorized emergency organization

ICS seeks to address the deficiencies identified by FIRESCOPE by establishing a management structure comprising five divisions: Command, Logistics, Operations, Planning, and Administration and Finance. A sixth division, Intelligence and Investigation, may be added to the command structure as dictated by the incident. All personnel within these functional areas need a complete understanding of NIMS and ICS to ensure optimum performance during and after an emergency. Figure 1 presents a simple ICS command structure.

ICS is designed to achieve nine major goals, which are summarized below.

1. Unity of Command

Each individual participating in the operation reports to only one supervisor, thus eliminating the potential for conflicting orders. The advantages of unity of command are that it provides accountability, prevents freelancing, improves the flow of information, helps coordinate operational efforts, and enhances operational safety. Unity of command is fundamental to the ICS chain of command structure.

2. Common Terminology

Prior to ICS, individual response agencies often developed plans, protocols, and procedures individually. The terminology used by one agency sometimes had different meanings for others, which caused confusion.

When different organizations are required to work together, common terminology is essential for cohesion, both within and between organizations responding to the incident.

ICS promotes the use of a common terminology and has a glossary of terms that brings consistency to position titles, the description and organization of resources, the type and names of incident facilities, and a host of other subjects. The use of common terminology is most evident in the titles of command roles, such as Incident Commander (IC), Safety Officer, and Operations Section Chief.

3. Management by Objective

Emergency incidents are managed by aiming toward specific objectives. For example, in a confined space rescue, multiple objectives such as ventilation, entry, and patient packaging may be required for success. Each objective is ranked by priority. The objectives should be as specific as possible and achievable within the working time frame. Objectives are accomplished by first outlining strategies and then determining appropriate tactics for executing them.

4. Flexible and Modular Organization

Incident Command structure can expand and contract according to the incident scope, resources, and hazards. Command is established in a top-down fashion, starting with the most important and authoritative positions. For example, Incident Command is established by the unit that arrives first at the scene of the incident.

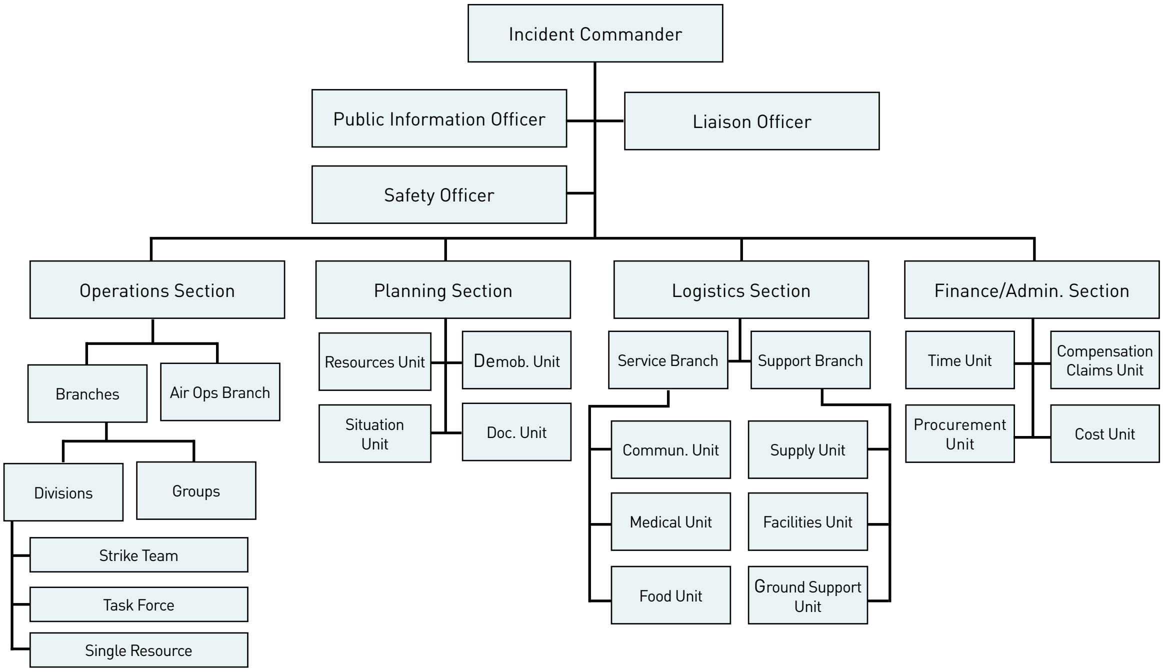
Only positions that are required at any given time within the incident should be established. In many cases, only a few positions within the command structure may need to be activated, or multiple roles may be completed by a single person. For example, a small chemical spill within a facility might be managed by the OEHS professional serving as the IC with no other roles required.

As an incident grows in size or complexity, ICS can be expanded. The largest and most complex incidents require the filling of the entire ICS staff. As the incident is managed, staffing is reduced until the IC is the only remaining staffed position and the event is terminated.

5. Span of Control

"Span of control" refers to the number of subordinates and resources that a single person can manage. ICS has established that each position within the command structure maintain a span of control between three and seven subordinates, with five being optimal. Requiring a single person to supervise more than seven others will result in overloading. In such a situation, the management structure should be expanded to reduce the number of resources to

Figure 1. A simplified ICS command structure. Source: FEMA, **bit.ly/femaicsreview** (PDF).



the optimum of five by establishing new teams and units as needed. When the span of control is reduced to fewer than three subordinates, the resources may be absorbed into the next level of command.

6. Coordination
Coordination is facilitated by implementing incident action plans, managing resources in a comprehensive manner, and integrating communications. One of the benefits of ICS is that it promotes coordination between organizations that otherwise work together sporadically. Coordination allows for flexibility within ICS and adds expertise by utilizing a range of organizations. However, this networking of ICS organizations can create management challenges. Some participants in incident responses have noted that ICS provides greater benefits when working relationships and training already exist between coordinating organizations. Incidents where working relationships do not already exist typically have more issues with authority and unity of command.

7. Incident Action Plans
Incident action plans, an integral component of ICS, document the goals, operational timeframe (typically no more than 12 hours), and response strategy developed in the planning process. IAPs for hazardous materials incidents must be written; for other incidents, IAPs may be verbal. The U.S. Department of Health and Human Services website at **bit.ly/dhhsiap** identifies the elements that should be included in an IAP.

8. Comprehensive Resource Management
Comprehensive resource management must be established to ensure that all resources, including physical assets and personnel, are identified, tracked, and accounted for from the inception of the event until they are returned to service. Resources *must* be tracked and managed properly to prevent failure of the incident action plan.

Resources need to be continuously monitored so they can be effectively deployed during an incident and systematically demobilized as an event is terminated. Assets are categorized as either “staged/available,” for resources that may be assigned; “committed/assigned,” for resources that are actively engaged in supervised field activities; or “out of service,” for resources that currently are neither assigned nor in staging. Resources may be out of service for reasons such as the restocking of supplies, personnel downtime, or damage to equipment.

9. Integrated Communications
The ability to communicate effectively is key to the success of an incident response and must be considered early in the planning process. Many agencies that responded to the 9/11 terrorist attacks were unable to communicate through an integrated communication system.

An integrated voice and data communications system, including equipment, systems, and protocols, must be developed prior to an incident. Effective ICS communications include three elements: modes, or the hardware systems that transfer information; planning, which accounts for the use of all available communications resources; and networks, which are procedures and processes for transferring information.

NATIONAL INCIDENT MANAGEMENT SYSTEM

Prior to the inception of NIMS, ICS was the primary response management system in the U.S. Its use was usually restricted to typical emergency response agencies such as fire, police, and EMS, but many other agencies, such as the U.S. Coast Guard, had also adopted ICS. In February 2003, President Bush issued Homeland Security Presidential Directive 5, or HSPD-5, which required the development of a single national incident management system to be used by all federal, state, and local emergency response agencies. For the first time, the system would include government agencies as well as business, education, and other shareholder communities.

The three guiding principles of NIMS are flexibility, standardization, and unity of efforts. These guiding principles are supported by the six basic components discussed below.

1. Command and Management
The successful command and management of any incident uses the following attributes:
- common terminology
- modular organization
- management by objectives
- incident action planning
- manageable span of control
- incident facilities and locations
- comprehensive resource management
- integrated communications
- establishment and transfer of command
- unified command
- chain of command and unity of command
- accountability
- dispatch and deployment
- information and intelligence management

This framework often determines the overall success or failure of the response. Many other components of NIMS and ICS also depend on this framework to ensure the proper response to an incident.

2. Preparedness
All incident management systems begin with preparedness, and NIMS is no exception. The first step in preparedness is recognizing that a risk exists and will require a response. This risk may be as simple as a confined space rescue or as complex as an incident spanning numerous states over an extended period. Preparedness requirements include but may not be limited to conducting hazard evaluation and risk assessments, developing policy, planning, training, equipping, exercising, evaluating, reviewing after the incident has terminated, and developing corrective action plans.

Preparation involves resource management. Resources include but are not limited to personnel, equipment, supplies, teams, and facilities.

3. Resource Management

Once the planning stage has been completed, resources need to be acquired, stored, inventoried, and maintained. Resource management involves inventorying and tracking assets. Inventoried assets are those whose use is reserved for a specific incident; other assets are used on a regular basis and therefore may not be available. Resource management must also account for items such as batteries, calibration supplies, and medical equipment, which may require replenishment during the incident response phase.

Whether resources are utilized on a day-to-day basis or stored for a specific response, NIMS plans should identify the following:

- What resources are readily available, widely used, and sharable?
- Where are the resources located? Are they local, state, or national?
- What is each resource's capability, category, type, and kind?
- Are the resources compatible or interoperable?

To ensure that personnel resources are maintained and mission ready, consider their qualifications, certifications, and credentials.

4. Communications and Information Management

Standardized communications, including the use of plain language and common terminology, will ensure that information exchanged among agencies is effective, concise, and efficient. The interoperability of communications technologies, policies, procedures, and systems must be established to maintain the flow of information.

Communications and information management is not limited to the response agencies; it must include the public and other impacted sectors. To be effective, information must be factual, timely, properly disseminated, and managed. Failure of communications and information management frequently leads to myriad problems such as freelancing, duplication of efforts, improper documentation, delay of asset deployment, and the spread of rumors.

5. Supporting Technologies

The disruptions to technologies during 9/11 illustrated the need for supporting technologies to include alternatives for systems susceptible to damage or disruption. Available technologies that can support and improve operations must be included as part of the NIMS process. Examples of these technologies include voice communications, data communications, GPS, information management systems, recordkeeping, asset tracking and inventorying, personnel management systems, and information distribution systems.

The technologies utilized should be cost effective, interoperable, easily supportable, and aligned with current technology standards.

6. Ongoing Management and Maintenance

Of key importance is the ongoing maintenance and management of all plans, personnel, training, recordkeeping, and resources. Even a well-planned response will fail if resources are not available when required. For information about the management and maintenance tasks required to maintain NIMS compliance, see **dhs.gov** and **fema.gov**.

TRAINING

This article provides a broad overview of the ICS and NIMS management systems. Becoming an integral part of an incident response requires training and education. Training for NIMS can be obtained from the Federal Emergency Management Agency at the National Fire Academy. At a minimum, a person who will be preparing or responding to incidents must complete the NIMS 100 course, Introduction to the Incident Command System, and NIMS 700, Introduction to the National Incident Management System. Additional courses regarding NIMS and ICS can also be taken at **bit.ly/trainingfema**.

PREPARATION AND PLANNING

Regardless of the industry or sector they are employed in, OEHS and IH professionals who prepare, plan, and respond to incidents must comply with HSPD-5, ICS, and NIMS. Together with the first response community; local, state, and federal government agencies; nongovernmental organizations; and others, we must properly plan for and respond to incidents. Doing so will result in a greater probability that responses protect property and the environment, and, most importantly, reduce injuries and the loss of life. Ⓢ

KENNETH C. ECK, CIH, CSP, CFPS, CHMM, DABFE, FACFEI, LEED AP, is director of EHS/IH/Educational Services at Quality Environmental Solutions & Technologies Inc. He can be reached at **keck@qualityenv.com**.

Send feedback to **synergist@aiha.org**.

RESOURCES

California Department of Forestry and Fire Protection: "The Incident Command System: A 25 Year Evaluation by California Practitioners," **bit.ly/ics25eval** (February 2000).

Department of Homeland Security: Homeland Security Presidential Directive 5, **bit.ly/hspd5** (February 2003).

Department of Homeland Security: "Public Health Emergency: What Is an Incident Action Plan?" **bit.ly/dhhsiap**.

Emergency Management Services International: "History of ICS," **bit.ly/emsiicshistory**.

Emergency Management Services International: "Summary of Changes to 2017 NIMS," **bit.ly/emsi2017nims**.

Federal Emergency Management Agency: "ICS Review Document, Extracted From -E/L/G 0300 Intermediate Incident Command System for Expanding Incidents, ICS 300," **bit.ly/femaicsreview** (PDF, March 2018).

Federal Emergency Management Agency: Introduction to the Incident Command System, (ICS 100.b) Student Manual (August 2010).

Federal Emergency Management Agency: IS-700.A: National Incident Management System, An Introduction, Student Manual (January 2009).

Regional Fire Analysis Report, Laguna Fire, September 26, 1970, Cleveland National Forest, **bit.ly/lagunareport** (PDF).