

IS-700 National Incident Management System, an Introduction Executive Summary

On February 28, 2003, President Bush issued Homeland Security Presidential Directive-5 (HSPD-5) directing the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). NIMS provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents. The intent of NIMS is to improve coordination and cooperation between public and private entities in a variety of domestic incident management activities.

Beginning in Federal Fiscal Year (FFY) 2005, the Department of Homeland Security (DHS) requires a phased-in adoption and implementation of NIMS by State and local governments as a condition of receipt of Federal preparedness funds. State and local governments must fully implement NIMS by FFY 2006. NIMS will not replace California's current incident management system, the Standardized Emergency Management System (SEMS) rather, NIMS will be integrated into SEMS.

NIMS Concepts and Principles

NIMS provides a framework for interoperability and compatibility by balancing flexibility and standardization. NIMS provides a flexible framework that provides a comprehensive, national approach to incident management applicable across all jurisdictional levels and functional disciplines, regardless of incident cause, size, location, or complexity.

NIMS Components

NIMS is comprised of six components that work together as a system to provide a national framework for preparing for, preventing, responding to, and recovering from domestic incidents. These components include:

- Command and management.
- Preparedness.
- Resource management.
- Communications and information management.
- Supporting technologies.
- Ongoing management and maintenance.

Command and Management

NIMS standard incident management structures are based on three key organizational systems:

1. **Incident Command System (ICS):** Defines the operating characteristics, management components, and structure of incident management organizations. ICS is based on “best practices”. ICS features include:
 - Common terminology: Standardized titles for facilities and positions. Standard terminology helps reduce confusion between the day-to-day position occupied by an individual and his/her position at the incident.
 - Span of control: Effective span of control may vary from three to seven; NIMS recommends a ratio of one supervisor to five reporting elements.
 - Incident Action Plan (IAP): IAPs provide a coherent means to communicate the overall incident objectives in the context of operational and support activities. IAPs are based on “management by objectives” to accomplish response tactics.

In some situations, NIMS recommends variations in incident management. The two most common variations involve the use of Unified Command and Area Command.

- *Unified Command* is an application of ICS when there is more than one responding agency with responsibility for the incident, or for incidents crossing political jurisdictions. For example, the fire department, water authority, and local environmental authority may each participate in a Unified Command for a hazardous materials spill that contaminates a nearby reservoir.
 - *Area Command* is an organization established to oversee the management of multiple incidents managed by an ICS organization, or large incidents that cross jurisdictional boundaries. Area Commands are particularly relevant to public health emergencies that are geographically dispersed and evolve over time. Because operations are conducted on-scene, there is no Operations Section in an Area Command.
2. **Multiagency Coordination Systems:** Defines the operating characteristics and organizational structure of supporting entities for large or wide-scale emergencies requiring higher-level resource management or information management. One key function of Multiagency Coordination Systems is making resource allocation decisions based on incident management priorities. Direct tactical and operational responsibility for the conduct of incident management activities rests with the on-scene Incident Commander.

Multiagency Coordination Systems include Emergency Operations Centers (EOCs) and, in certain multijurisdictional or complex incidents, Multiagency Coordination Entities.

- EOCs support multiagency coordination and joint information activities.
 - *Multiagency Coordination Entities* typically consist of principals from organizations with significant incident management support/resource responsibilities.
3. **Public Information Systems:** Defines the processes and procedures for communicating timely and accurate information to the public during emergencies. The Public Information Officer (PIO) advises the Incident Commander on all public

information matters related to the management of the incident. The PIO follows Joint Information System (JIS) protocols to coordinate public information at all levels.

Incident Commanders and Multiagency Coordination Entities may establish a Joint Information Center (JIC) to ensure the coordination of public information. In the case of a Unified Command, those contributing to joint public information management retain their organizational independence. When multiple JICs are established, all JICs must communicate and coordinate with each other on an ongoing basis using established JIS protocols.

Preparedness

Preparedness includes all actions required to establish the level of capability necessary to execute incident management operations. Two key functions of preparedness organizations are to: (1) coordinate preparedness plans; and (2) adopt guidelines and protocols for resource management. Preparedness involves a combination of:

- Planning, including Corrective Action Plans based on lessons learned.
- Training/exercises.
- Timely delivery of assistance during incidents using mutual aid agreements and Emergency Management Assistance Compacts.

Resource Management

Resource management under NIMS is based on “resource typing”, that is, categorizing resources based on measurable standards of capability and performance (500-kw generator). NIMS also requires personnel certification and credentialing standards to ensure minimum level of skills, knowledge and experience necessary to perform tasks.

Since resource requirements and availability will change as the incident evolves, all entities must coordinate closely. The Incident Commander must submit requests for items that cannot be obtained locally through a Multiagency Coordination System using standardized procedures. NIMS defines standardized mechanisms for describing, inventorying, mobilizing, dispatching, tracking resources from mobilization to demobilization, and recovering resources over the life cycle of an incident.

Communications and Information Management

NIMS identifies requirements for a standardized framework for communications, information management, and information-sharing support at all levels of incident management. Communications and information management under NIMS is based on a common operating picture necessary to ensure consistency at all levels, among all who respond to or manage incident response.

Ongoing Management and Maintenance

Federal DHS established the NIMS Integration Center (NIC) to provide strategic direction and oversight in support of ongoing NIMS review and refinement. NIC responsibilities include:

- Maintain and manage national-level preparedness standards related to NIMS.
- Define general training requirements and approved training courses for all NIMS users.
- Review and approve emergency responder equipment lists that meet national standards.