NIMS *Basic*

FEMA 501-5
March 29, 2006
Revision 0

Communications and Information Management

I. Purpose:

This document describes a framework for establishing a common operating picture and systems interoperability for incident management.

II. Scope:

Prior to an incident, entities responsible for taking appropriate pre-incident actions use communications and information management processes and systems to inform and guide various critical activities. These actions include:

- Mobilization or pre-deployment of resources.
- Strategic planning by:
  - Preparedness organizations.
  - Multi-agency coordination entities.
  - Agency executives.
  - Jurisdictional authorities.
  - EOC personnel.

During an incident, incident management personnel use communications and information processes and systems to inform the preparedness organizations, multiagency coordination entities, agency executives, jurisdictional authorities, and EOC personnel of the formulation, coordination, and execution of operational decisions and requests for assistance.

A. Goals

Critical aspects of domestic incident management are:

- Effective communications.
- Information management.
- Information and intelligence sharing.

Principal goals of communications and information management are:

- Establishing and maintaining a common operating picture
- Ensuring accessibility and interoperability.

B. Information Use

A common operating picture and systems interoperability provide the information necessary to:

- Formulate and disseminate indications and warnings.
- Formulate, execute, and communicate operational decisions at an incident site, as well as between incident management entities across jurisdictions and functional agencies.
- Prepare for potential requirements and requests supporting incident management activities.
- Develop and maintain overall awareness and understanding of an incident within and across jurisdictions.

C. NIMS Basic

This series of documents is extracted from FEMA 501, *National Incident Management System* and contains a bullet item reformat of text extracted from the original document. Each document is one chapter or appendix from the NIMS, and uses the same wording to allow easy comparison of the documents. Always refer to the NIMS in case of questions or conflicting information.

NIMS Basic is organized with the purpose, scope, and definitions at the front of the document. The Process section follows and contains the main body of the document. References and supersedure information are at the end.

III. Table of Contents:

I. Purpose: 1
II. Scope: 1
A. Goals 1
B. Information Use 2
C. NIMS Basic 2
III. Table of Contents: 2
IV. Definitions: 3
V. Process: 3
A. Concepts and Principles 3
1. Common Operating Picture 3
2. Communications and Data Standards 3
B. Managing Information and Communications 3
1. Incident Management Communications 4
2. Information Management 4
3. Interoperability Standards 5
VI. References: 6
VII. Supersedure: 6

IV. Definitions:

EOC	Emergency Operations Center
NIC	NIMS Integration Center
NIMS	National Incident Management System

V. Process:

A. Concepts and Principles

Sustained collaborative effort over time will result in progress toward common communications, and data standards and systems interoperability.

1. Common Operating Picture

Use integrated systems for communication, information management, and intelligence and information sharing to continuously update data during an incident. This provides a common framework that covers the incident life cycle across jurisdictions and disciplines.

A common operating picture accessible across jurisdictions and functional agencies:

- Allows incident managers at all levels to make effective, consistent decisions in a timely manner.
- Helps ensure consistency at all levels of incident management across jurisdictions, as well as between various engaged governmental jurisdictions, and private sector and non-governmental entities.

2. Communications and Data Standards

Fundamentals for an effective NIMS.

- Common communications and data standards.
- Related testing and compliance mechanisms.
- Communications interoperability in the context of incident management.

Adherence to standards also enhances effective communications outside the incident structure for resources and other support between:

- Other levels of government.
- Government and private entities.

B. Managing Information and Communications

NIMS communications and information systems enable the essential functions needed to provide a common operating picture and interoperability for incident management at all levels in two ways.

- Incident management communications.
- Information management.

1. Incident Management Communications

Preparedness organizations must ensure that effective communications processes systems exist to support a complete spectrum of incident management activities. The following principles apply:

- Individual jurisdictions will be required to comply with national interoperable communications standards when such standards are developed. The NIC will designate standards appropriate for NIMS users.
- Incident communications will follow the standards called for under ICS.
- The incident command manages communications at an incident, using a common communications plan and an incident-based communications center established solely for use by the command, tactical, and support resources assigned to the incident. All entities involved in managing the incident will utilize common terminology for communications prescribed by the NIMS.

2. Information Management

The NIC will facilitate the definition and maintenance of documented policies and interoperability standards required to guide the development of NIMS-related information systems.

a) Pre-Incident Information

The preparedness organizations described in NIC Document FEMA 501-3, *NIMS Basic - Preparedness*, in concert with private sector and non-governmental organizations, primarily meet the pre-incident information needs at the Federal, State, local, and tribal levels.

b) System

The information management system provides guidance, standards, and tools to enable Federal, State, local, tribal, and private sector and non-governmental entities to integrate their information needs into a common operating picture.

c) Networks

An EOC uses a combination of networks to disseminate critical information that constitutes a common operating picture, including:

- Indications and warnings.
- Incident notifications.
- Public communications.

Notifications are made to the appropriate jurisdictional levels and to private sector and nongovernmental organizations through the mechanisms defined in emergency operations and incident action plans at all levels of government.

d) Technology Use

Agencies must plan in advance for the effective and efficient use of information management technologies such as computers and networks in order to:

- Tie together all command, tactical, and support units involved in incident management.
- Enable these entities to share information critical to mission execution and the cataloguing of required corrective actions.

3. Interoperability Standards

Refer to NIC Document FEMA 501-7, *NIMS Basic - Ongoing Management and Maintenance*. The NIC will:

- Facilitate the development of data standards, to include secure communications when required, for the functions described below.
- Develop Standards in accordance with the following sections.

a) Incident Notification/ Situation Report

Incident notification takes place at all levels.

- Standardize notification and situation report data, but not prevent information unique to a reporting organization from being collected or disseminated.
- Standardize the transmission of data in a common format to enable the passing of appropriate notification information to a national system where data queries and information/intelligence assessments and analysis can occur.

b) Status Reporting

Define a standard set of data elements to facilitate the process for all levels of government to initiate status reports, and then disseminate them to other jurisdictions.

Example: Situation Reports (SITREPS) and Pollution Reports (POLREPS).

c) Analytical Data

Multiple organizations at different levels of government often respond and collect data during incidents that require public health and environmental sampling.

- Standardize sampling and data collection to enable more reliable laboratory analysis and improve the quality of assessments provided to decision makers.
- Collect analytical data in the field, such as information on public health and environmental monitoring, in a manner that observes standard data definitions.
- Transmit the data to laboratories using standardized analysis processes.

d) Geospatial Information

Correct utilization of geospatial data is increasingly important to decision makers.

- Geospatial information is used to integrate assessments, situation reports, and incident notification into a coherent common operating picture.
- Tie the use of geospatial data to consistent standards to prevent incorrectly transformed or otherwise misapplied coordinates to cause inconspicuous, yet serious errors.
- Robust standards covering geospatial information should enable systems to be used in remote field locations where telecommunications capabilities may not have sufficient bandwidth to handle large images or are limited in terms of computing hardware.

e) Wireless Communications

The NIMS will include standards for interoperable wireless communications and computing for Federal, State, tribal, and local public safety organizations and non-governmental organizations to ensure that incident management organizations can communicate and share information with each other through wireless systems.

f) Identification and Authentication

Individuals and organizations that access the NIMS information management system, and in particular, those that contribute information to the system, such as situation reports, must be properly authenticated and certified for security purposes.

This requires a national authentication and security certification standard for the NIMS that is flexible and robust enough to ensure that information can be properly authenticated and protected.

- The NIC is responsible for facilitating the development of these standards.
- Different levels of government and private organizations must collaborate to administer the authentication process.

g) National Database of Incident Reports

Federal, State, tribal, and local organizations responsible for receiving initial incident reports will work collaboratively through the NIC to develop and adopt a national database of incident reports that can be used to support incident management efforts.

VI. References:

FEMA 501, *National Incident Management System*

FEMA 501-3, *NIMS Basic - Preparedness*

FEMA 501-7, *NIMS Basic - Ongoing Management and Maintenance*

VII. Supersedure:

Original