

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

Effective emergency management and incident response activities rely on flexible communications and information systems that provide a common operating picture to emergency management/response personnel¹⁰ and their affiliated organizations. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are the principal goals of the Communications and Information Management component of NIMS. Properly planned, established, and applied communications enable the dissemination of information among command and support elements and, as appropriate, cooperating agencies and organizations.

Incident communications are facilitated through the development and use of common communications plans and interoperable communications equipment, processes, standards, and architectures. During an incident, this integrated approach links the operational and support units of the various organizations to maintain communications connectivity and situational awareness. Communications and information management planning should address the incident-related policies, equipment, systems, standards, and training necessary to achieve integrated communications.

A. CONCEPTS AND PRINCIPLES

The underlying concepts and principles of this component reinforce the use of a flexible communications and information system in which emergency management/response personnel can maintain a constant flow of information during an incident. These concepts and principles emphasize the need for and maintenance of a common operating picture; interoperability; reliability, scalability, and portability; and resiliency and redundancy of any system and its components.

1. COMMON OPERATING PICTURE

A common operating picture is established and maintained by gathering, collating, synthesizing, and disseminating incident information to all appropriate parties. Achieving a common operating picture allows on-scene and off-scene personnel—such as those at the Incident Command Post, Emergency Operations Center (EOC), or within a Multiagency Coordination Group—to have the same information about the incident, including the availability and location of resources and the status of assistance requests. Additionally, a common operating picture offers an incident overview that enables the Incident Commander (IC),

Common Operating Picture

An overview of an incident created by collating and gathering information—such as traffic, weather, actual damage, resource availability—of any type (voice, data, etc.) from agencies/organizations in order to support decisionmaking

¹⁰ Emergency management/response personnel include Federal, State, territorial, tribal, substate regional, and local governments, nongovernmental organizations, private-sector organizations, critical infrastructure owners and operators, and all other organizations and individuals who assume an emergency management role.

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

Unified Command (UC), and supporting agencies and organizations to make effective, consistent, and timely decisions. In order to maintain situational awareness, communications and incident information must be updated continually. Having a common operating picture during an incident helps to ensure consistency for all emergency management/response personnel engaged in an incident.

2. INTEROPERABILITY

Communications interoperability allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video in real time, when needed, and when authorized. It is essential that these communications systems be capable of interoperability, as successful emergency management and incident response operations require the continuous flow of critical information among jurisdictions, disciplines, organizations, and agencies.

Interoperability planning requires accounting for emergency management and incident response contingencies and challenges. Interoperability plans should include considerations of governance, standard operating procedures (SOPs), technology, training and exercises, and usage within the context of the stress and chaos of a major response effort. Coordinated decisionmaking between agencies and jurisdictions is necessary to establish proper and coherent governance and is critical to achieving interoperability. Agreements and SOPs should clearly articulate the processes, procedures, and protocols necessary to achieve interoperability.

3. RELIABILITY, SCALABILITY, AND PORTABILITY

Communications and information systems should be designed to be flexible, reliable, and scalable in order to function in any type of incident, regardless of cause, size, location, or complexity. They should be suitable for operations within a single jurisdiction or agency, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement. Communications systems should be applicable and acceptable to users, readily adaptable to new technology, and reliable in the context of any incident to which emergency management/response personnel would be expected to respond.

Portability of radio technologies, protocols, and frequencies among emergency management/response personnel will allow for the successful and efficient integration, transport, and deployment of communications systems when necessary. Portability includes the standardized assignment of radio channels across jurisdictions, which allows responders to participate in an incident outside their jurisdiction and still use familiar equipment.

Scalability differs from portability in that scalability allows responders to increase the number of users on a system, while portability facilitates the interaction of systems that are normally distinct.

4. RESILIENCY AND REDUNDANCY

Resiliency is the ability of communications systems to withstand and continue to perform after damage or loss of infrastructure. It requires communications systems to avoid relying solely on a sophisticated but vulnerable network of support systems. Prudent resiliency practices could include hardened dispatch centers and transmission systems or infrastructure that can withstand known risks. Repeater antenna sites, for example, are

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

equipped with independent power systems to ensure their continued functionality during a power failure.

Redundancy is another essential element of a jurisdiction's/organization's communications structure. Although the duplication of identical services is one method of achieving redundancy, it also derives from the ability to communicate through diverse, alternative methods when standard capabilities suffer damage. For example, a public safety agency might have a high-tech voice 400-megahertz system that is used as the primary dispatch system, but maintain a redundant VHF system in its vehicles that would be able to contact the dispatch center in the event that the primary system is rendered inoperable. Resiliency and redundancy are critical to ensuring communications flow during an incident.

B. MANAGEMENT CHARACTERISTICS

Emergency management/response personnel should be able to manage incident communications and information effectively. Regardless of the communications method or the information being transmitted, procedures and protocols should be followed. As technologies change and the methods of exchanging information improve, management procedures likewise should evolve.

1. STANDARDIZED COMMUNICATION TYPES

Successful communications and information management require that emergency management/response personnel and their affiliated organizations use standardized communications types. The determination of the individual or agency/organization responsible for these communications is discussed in the Command and Management component and in Appendix B. The following is a list of standardized communication types:¹¹

- **Strategic Communications:** High-level directions, including resource priority decisions, roles and responsibilities determinations, and overall incident response courses of action.
- **Tactical Communications:** Communications between command and support elements and, as appropriate, cooperating agencies and organizations.
- **Support Communications:** Coordination in support of strategic and tactical communications (for example, communications among hospitals concerning resource ordering, dispatching, and tracking from logistics centers; traffic and public works communications).
- **Public Address Communications:** Emergency alerts and warnings, press conferences, etc.¹²

2. POLICY AND PLANNING

Coordinated communications policy and planning provides the basis for effective communications and information management. Although communications and information management is important during routine operations, well-established procedures and protocols become critical during incident response activities. Careful planning should

¹¹ See page 70, Component IV: Command and Management, Public Information, and page 103, Appendix B: Incident Command System, Planning Section Chief.

¹² See page 70, Component IV, Command and Management, Public Information.

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

determine what communications systems and platforms will be used, who can use them, what information is essential in different environments, the technical parameters of all equipment and systems, and other relevant considerations.

Information flow among all stakeholders is crucial, but interoperability presents additional challenges when nongovernmental organizations (NGOs), the private sector, and critical infrastructure owners and operators are considered. All relevant stakeholders should be involved in meetings and planning sessions in order to formulate more thorough and integrated communications plans and strategies. Technology and equipment standards also should be shared when appropriate, to provide stakeholders with the opportunity to be interoperable and compatible.

Sound communications management policies and plans should include information about the following aspects of communications and information management:

- Information needs should be defined by the jurisdiction/organization. These needs are often met at the Federal, State, tribal, and local levels, in concert with NGOs and the private sector, and primarily through preparedness organizations.
- The jurisdiction's or organization's information management system should provide guidance, standards, and tools to enable the integration of information needs into a common operating picture when needed.
- Procedures and protocols for the release of warnings, incident notifications, public communications, and other critical information are disseminated through a defined combination of networks used by EOCs. Notifications are made to the appropriate jurisdictional levels and to NGOs and the private sector through defined mechanisms specified in emergency operations plans and Incident Action Plans.
- Agencies at all levels should plan in advance for the effective and efficient use of information management technologies (e.g., computers, networks, and information-sharing mechanisms) to integrate all command, coordination, and support functions involved in incident management and to enable the sharing of critical information and the cataloging of required corrective actions.

3. AGREEMENTS

All parties identified in the planning process used in a jurisdiction's emergency operations plan need to have agreements in place to ensure that the elements within plans and procedures will be in effect at the time of an incident. The agreements should specify all of the communications systems and platforms through which the parties agree to use or share information.

4. EQUIPMENT STANDARDS AND TRAINING

Communications equipment used by emergency management/response personnel often consists of components and systems that may be connected through common interfaces, many of which rely on the private sector to provide their operational backbone. Public/private communication systems and associated equipment should be regularly enhanced and updated, as their maintenance is essential to effective emergency management and incident response activities. The wide range of conditions under which communications systems will be used should be considered when developing standards

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

associated with the systems and equipment. Training and exercises that employ interoperable systems and equipment are necessary for personnel to understand their capabilities and limitations before an incident. In addition, the need for “hardened” laptops and/or personal digital assistants should be considered in the communications plan.

C. ORGANIZATION AND OPERATIONS

1. INCIDENT INFORMATION

During the course of an incident, information is vital to assist the IC, UC, and supporting agencies and organizations in making decisions. Much of the information is used for diverse functions within the Incident Command System. For example, the same piece of information may:

- Aid in the planning process to develop an Incident Action Plan (IAP).
- Be a key point in the release of public information.
- Assist the Finance/Administration Section in determining incident cost.
- Determine the need for additional involvement of NGO or private-sector resources.
- Identify a safety issue.
- Follow up on an information request.

The following are examples of information generated by an incident that can be used for decisionmaking purposes.

a. Incident Notification, Situation, and Status Reports

Incident reporting and documentation procedures should be standardized to ensure that situational awareness is maintained and that emergency management/response personnel have easy access to critical information. Situation reports offer a snapshot of the past operational period and contain confirmed or verified information regarding the explicit details (who, what, when, where, and how) relating to the incident. Status reports, which may be contained in situation reports, relay information specifically related to the status of resources (e.g., availability or assignment of resources).

The information contained in incident notification, situation, and status reports must be standardized in order to facilitate its processing; however, the standardization must not prevent the collection or dissemination of information unique to a reporting organization. Transmission of data in a common format enables the passing of pertinent information to appropriate jurisdictions and organizations and to a national system that can handle data queries and information/intelligence assessments and analysis.

b. Analytical Data

Data, such as information on public health and environmental monitoring, should be collected in a manner that observes standard data collection techniques and definitions. The data should then be transmitted using standardized analysis processes. During incidents that require public health and environmental sampling, multiple organizations at different levels of government often collect data, so standardization of data collection and analysis is critical. Additionally, standardization of sampling and data collection enables more reliable analysis and improves the quality of assessments provided to decisionmakers.

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

c. Geospatial Information

Geospatial information is defined as information pertaining to the geographic location and characteristics of natural or constructed features and boundaries. It is often used to integrate assessments, situation reports, and incident notification into a common operating picture and as a data fusion and analysis tool to synthesize many kinds and sources of data and imagery. The use of geospatial data (and the recognition of its intelligence capabilities) is increasingly important during incidents. Geospatial information capabilities (such as nationally consistent grid systems or global positioning systems based on lines of longitude and latitude) should be managed through preparedness efforts and integrated within the command, coordination, and support elements of an incident, including resource management and public information.

The use of geospatial data should be tied to consistent standards, as it has the potential to be misinterpreted, transposed incorrectly, or otherwise misapplied, causing inconspicuous yet serious errors. Standards covering geospatial information should also enable systems to be used in remote field locations or devastated areas where telecommunications may not be capable of handling large images or may be limited in terms of computing hardware.

2. COMMUNICATIONS STANDARDS AND FORMATS

Communications and data standards, related testing, and associated compliance mechanisms are necessary to enable diverse organizations to work together effectively. These include a standard set of organizational elements and functions, common “typing” of resources to reflect specific capabilities, and common identifiers for facilities and operational locations used to support incident operations.¹³ Common terminology, standards, and procedures should be established and detailed in plans and agreements, where possible. Jurisdictions may be required to comply with national interoperable communications standards, once developed. Standards appropriate for NIMS users will be designated by the National Integration Center (NIC) in partnership with recognized standards development organizations.

a. Radio Usage Procedures

Procedures and protocols for incident-specific communications and other critical incident information should be set forth in agreements or plans prior to an incident, where possible. These procedures and protocols form the foundation for the development of the communications plan during an incident. The receiving center should be required to acknowledge receipt of the emergency information. Additionally, each agency/organization should be responsible for disseminating this information to its respective personnel.

All emergency management/response personnel participating in emergency management and incident response activities should follow recognized procedures and protocols for establishing interoperability, coordination, and command and control.

During incident response activities, radio traffic should be restricted to those messages necessary for the effective execution of emergency management/response personnel tasks.

¹³ See page 41, Component III: Resource Management, Identifying and Typing Resources.

COMPONENT II: COMMUNICATIONS AND INFORMATION MANAGEMENT

b. Common Terminology, Plain Language (Clear Text), Compatibility

The ability of emergency management/response personnel from different disciplines, jurisdictions, organizations, and agencies to work together depends greatly on their ability to communicate with each other. Common terminology enables emergency management/response personnel to communicate clearly with one another and effectively coordinate activities, no matter the size, scope, location, or complexity of the incident.

The use of plain language (clear text) in emergency management and incident response is a matter of public safety, especially the safety of emergency management/response personnel and those affected by the incident. It is critical that all those involved with an incident know and use commonly established operational structures, terminology, policies, and procedures. This will facilitate interoperability across agencies/organizations, jurisdictions, and disciplines.

All communications between organizational elements during an incident, whether oral or written, should be in plain language; this ensures that information dissemination is timely, clear, acknowledged, and understood by all intended recipients. Codes should not be used, and all communications should be confined to essential messages. The use of acronyms should be avoided during incidents requiring the participation of multiple agencies or organizations. Policies and procedures that foster compatibility should be defined to allow information sharing among all emergency management/response personnel and their affiliated organizations to the greatest extent possible.

c. Encryption or Tactical Language

When necessary, emergency management/response personnel and their affiliated organizations need to have a methodology and the systems in place to encrypt information so that security can be maintained. Although plain language may be appropriate during response to most incidents, tactical language is occasionally warranted due to the nature of the incident (e.g., during an ongoing terrorist event). The use of specialized encryption and tactical language should be incorporated into any comprehensive IAP or incident management communications plan.

d. Joint Information System and Joint Information Center

The Joint Information System (JIS) and the Joint Information Center (JIC)¹⁴ are designed to foster the use of common information formats. The JIS integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, and timely information during crisis or incident operations.

The JIC provides a structure for developing and delivering incident-related coordinated messages. It develops, recommends, and executes public information plans and strategies; advises the IC, UC, and supporting agencies or organizations concerning public affairs issues that could affect a response effort; and controls rumors and inaccurate information that could undermine public confidence in the emergency response effort. It is the central point of contact for all news media at the scene of an incident. Public information officials from all participating agencies/organizations should co-locate at the JIC.

¹⁴ See pages 70–71, Component IV: Command and Management, Joint Information System and Joint Information Center.

e. Internet/Web Procedures

The Internet and other Web-based tools can be resources for emergency management/response personnel and their affiliated organizations. For example, these tools can be used prior to and during incidents as a mechanism to offer situational awareness to organizations/agencies involved in the incident or to the public, when appropriate.

The Internet and other Web-based tools can be used, as appropriate, during incidents to help with situational awareness and crisis information management.

Procedures for use of these tools during an incident should be established to leverage them as valuable communications system resources. Information posted or shared during an incident through these applications should follow planned and standardized methods and generally conform with the overall standards, procedures, and protocols.

f. Information Security

Procedures and protocols must be established to ensure information security. Inadequate information security can result in the untimely, inappropriate, and piecemeal release of information, which increases the likelihood of misunderstanding and can compound already complicated public safety issues. The release of inappropriate classified or sensitive public health or law enforcement information can jeopardize national security, ongoing investigations, or public health. Misinformation can place persons in danger, cause public panic, and disrupt the critical flow of proper information. Correcting misinformation wastes the valuable time and effort of incident response personnel.

Individuals and organizations that have access to incident information and, in particular, contribute information to the system (e.g., situation reports) must be properly authenticated and certified for security purposes. This requires a national authentication and security certification standard that is flexible and robust enough to ensure that information can be properly authenticated and protected. Although the NIC is responsible for facilitating the development of these standards, all levels of government, NGOs, and the private sector should collaborate on the authentication process.