
Unit 4: NIMS Communications and Information Management

This page intentionally left blank.

Objectives

At the end of this unit, you should be able to:

- Describe the importance of communications and information management.
 - Define the concepts of common operating picture and interoperability.
 - Describe the purpose of communications and information management standards, procedures, and protocols.
-

Scope

- Unit Introduction and Objectives
 - Video: What is NIMS Communications and Information Management?
 - Characteristics of Effective Communications Systems
 - Flexible Communications and Information Systems
 - Common Operating Picture
 - Interoperability
 - Reliability, Portability, Scalability
 - Resiliency and Redundancy
 - Activity
 - Standards, Procedures, and Protocols
 - Standardized Communications Types
 - Policy and Planning
 - Agreements
 - Equipment Standards and Training
 - Incident Information
 - Communications and Data Standards
 - Plain Language & Common Terminology
 - Knowledge Review and Summary
 - Preparedness Self-Assessment
-

This page intentionally left blank.



Key Points

This unit presents an overview of the NIMS Communications and Information Management component.

Unit Objectives

- Describe the importance of communications and information management.
- Define the concepts of common operating picture and interoperability.
- Describe the purpose of communications and information management standards, procedures, and protocols.

Unit List

- ✓ Overview
- ✓ Understanding NIMS
- ✓ Preparedness
- **Communications and Information Management**
- Resource Management
- Command and Management
- Additional Resources and Course Summary

See pages 23-30 of the NIMS document.

FEMA NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.2

Key Points

At the end of this unit, you should be able to:

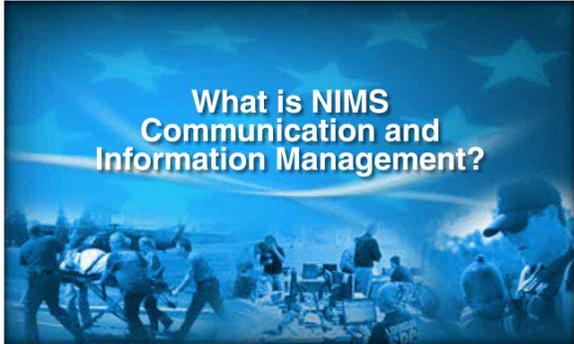
- Describe the importance of communications and information management.
- Define the concepts of common operating picture and interoperability.
- Describe the purpose of communications and information management standards, procedures, and protocols.

This unit summarizes the information presented in Component II: Communications and Information Management, including:

- Concepts and Principles
- Management Characteristics
- Organization and Operations

Refer to pages 23 through 30 of the NIMS document.

What Is NIMS Communications & Info Management?



Click on the image to start the video.

 **FEMA**

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.3

Key Points

This video provides an introduction to the NIMS Communications and Information Management component.

Video Transcript: Effective emergency response depends on communication—the ability to maintain a common operating picture through the constant flow of information.

During and after Hurricane Katrina, communications systems failed, severely hampering information flow and response operations. In New Orleans, most of the city was flooded. The combined effects of wind, rain, storm surge, breached levees, and flooding knocked out virtually the entire infrastructure—electrical power, roads, water supply and sewage, and communications systems.

Thomas Stone, Fire Chief, St. Bernard Parish: “We lost our communications system, and when you are not able to communicate, you can’t coordinate your response. You never think that you will lose your entire infrastructure.”

Communications problems are not limited to systems being destroyed or not functioning. Similar problems arise when agencies cannot exchange needed information because of incompatible systems. NIMS identifies several important features of public safety communications and information systems.

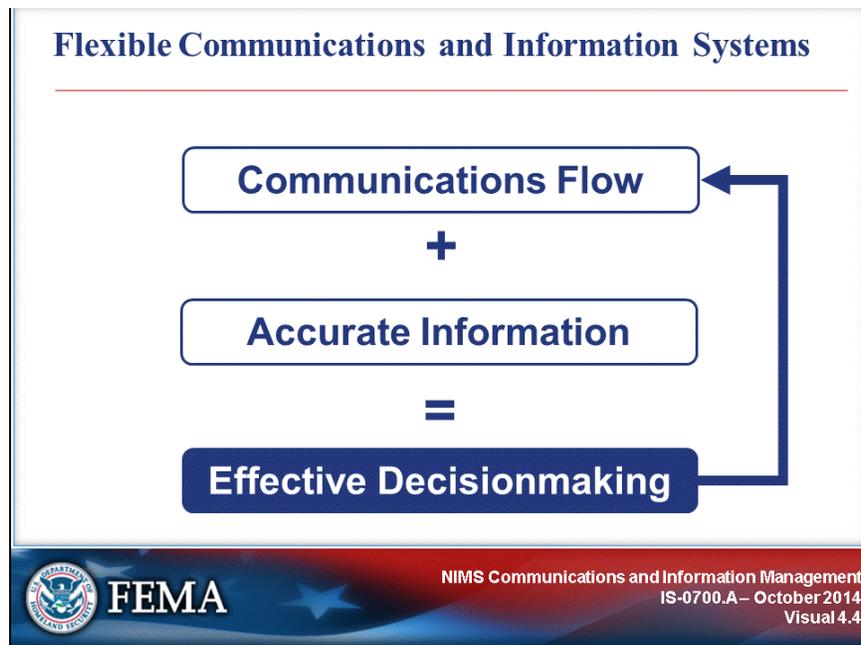
Communications systems need to be:

- **Interoperable**—able to communicate within and across agencies and jurisdictions.
- **Reliable**—able to function in the context of any kind of emergency.
- **Portable**—built on standardized radio technologies, protocols, and frequencies.
- **Scalable**—suitable for use on a small or large scale as the needs of the incident dictate.

- **Resilient**—able to perform despite damaged or lost infrastructure.
- **Redundant**—able to use alternate communications methods when primary systems go out.

Regardless of the communications hardware being used, standardized procedures, protocols, and formats are necessary to gather, collate, synthesize, and disseminate incident information. And in a crisis, life-and-death decisions depend on the information we receive.

This lesson introduces you to the NIMS Communications and Information Management component.



Key Points

All too often, after-action reports cite communications failures as an impediment to effective incident management.

Communications breakdowns are not limited to equipment and systems-related failures. The use of different protocols, codes instead of plain language, and nonstandardized reporting formats hampers our ability to share critical information and make effective decisions.

To overcome these past problems, the NIMS Communications and Information Management component promotes the use of flexible communications and information systems.

Common Operating Picture

A common operating picture:

- Is established and maintained by gathering, collating, synthesizing, and disseminating information.
- Allows on-scene and off-scene personnel to have the same information, including:
 - Availability and location of resources.
 - Status of assistance requests.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.5

Key Points

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, 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.

Interoperability

Emergency communications systems should:

- Be the same or linked to the same system used for nonemergency procedures.
- Effectively interface with national standards.
- Allow data sharing among key players.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.6

Key Points

First and foremost, **interoperability is the ability of emergency management/response personnel to interact and work well together.**

Interoperability also means that technical emergency communications systems should:

- Be the same or linked to the same system that the jurisdiction uses for nonemergency procedures.
- Effectively interface with national standards, as they are developed.
- Allow the sharing of data throughout the incident management process and among all key players.

Interoperability Saves Lives!

Consider the differences between the responses to the following incidents:

- 1982 Air Florida Flight 90 crash
- September 11, 2001, terrorist attack on the Pentagon



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.7

Key Points

The following examples to explain the value of interoperability:

Jan. 13, 1982: Air Florida Flight 90 crashed into the 14th St. Bridge in Washington, DC, during a snowstorm. More than 70 people lost their lives. Police, fire, and EMS crews responded quickly to the scene but experienced coordination problems because they could not communicate with one another.

Sept. 11, 2001: When American Airlines Flight 77 crashed into the Pentagon, 900 responders from 50 different agencies were able to communicate with one another. Response agencies had learned an invaluable lesson from the Air Florida tragedy. Regional coordination within the Washington area led to the adoption of the Incident Command System, establishment of interoperable communications protocols, and execution of mutual aid plans. The next challenge to solve was the lack of direct interoperability with secondary response agencies.

Reliability, Portability, Scalability

Communications systems should be:

- **Reliable** – able to function in any type of incident
- **Portable** – deployable to different locations and compatible with other systems
- **Scalable** – suitable for use on large or small scale



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.8

Key Points

To achieve interoperability, communications and information systems should be designed to be:

- **Reliable**—able to function in any type of incident, regardless of cause, size, location, or complexity.
- **Portable**—built on standardized radio technologies, protocols, and frequencies that allow communications systems to be deployed to different locations and integrated seamlessly with other systems.
- **Scalable**—suitable for use on a small or large scale, allowing for an increasing number of users.

Resiliency and Redundancy

Communications systems should have:

- **Resiliency** – ability to perform after damage or loss of infrastructure
- **Redundancy** – duplication of services or the ability to communicate through diverse, alternative methods



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.9

Key Points

Communications systems ensure that the flow of information will not be interrupted during an incident through:

- **Resiliency**—able to withstand and continue to perform after damage or loss of infrastructure.
- **Redundancy**—providing for either duplication of identical services or the ability to communicate through diverse, alternative methods when standard capabilities suffer damage.

Activity

Instructions:

1. Work with your group to answer the questions below.
2. Select a spokesperson and be prepared in 5 minutes.

Questions:

- What steps have you taken to ensure a common operating picture among response partners?
- What interoperability challenges have you faced and how have you addressed them?
- How do you ensure that communications systems are reliable, scalable, and portable?
- What are some best practices for ensuring communications systems are resilient and redundant?



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.10

Key Points

Instructions:

1. Work with your group to answer the questions below.
2. Select a spokesperson and be prepared in 5 minutes.

Questions:

- **What steps have you taken to ensure a common operating picture among response partners?**
- **What interoperability challenges have you faced and how have you addressed them?**
- **How do you ensure that communications systems are reliable, scalable, and portable?**
- **What are some best practices for ensuring communications systems are resilient and redundant?**

Standardized Communications Types

Successful communications and information management require the use of:

- Strategic communications
- Tactical communications
- Support communications
- Public address communications



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.11

Key Points

Successful communications and information management require that emergency management/response personnel and their affiliated organizations use the following types of standardized communications:

- **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.

The determination of the individual or agency/organization responsible for these communications is discussed in the NIMS Command and Management unit.

Policy and Planning

Communications plans should identify:

- **What** information is essential and can be shared.
- **Who** . . .
 - Needs the information.
 - Has the information.
- **How** . . .
 - Information will flow.
 - Information is coordinated for public and media release.
 - Communications systems will be used.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.12

Key Points

Coordinated communications policy and planning provide the basis for effective communications and information management.

All relevant stakeholders should be involved in planning sessions in order to formulate 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 the Emergency Operations Center. Notifications are made to the appropriate jurisdictional levels and to NGOs and the private sector through defined mechanisms specified in emergency operations 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.

Agreements

Agreements should:

- Be executed among all stakeholders.
- Specify communications systems and platforms to be used.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.13

Key Points

Agreements should be executed among all stakeholders to ensure that the elements within plans and procedures will be in effect at the time of an incident.

Agreements should specify all of the communications systems and platforms through which the parties agree to use or share information

Equipment Standards and Training

Standards should address:

- Conditions under which communications systems must operate
- Maintenance and updating of systems and equipment
- Periodic testing of systems



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.14

Key Points

Standards help ensure a seamless interface between communications systems, especially between the public and private sectors. Standards should address:

- The wide range of conditions under which communications systems must operate.
- The need for maintenance and updating of the systems and equipment.
- The periodic testing of systems.

Periodic training and exercises are essential so that personnel capabilities and limitations of communications plans and systems are addressed before an incident.

Incident Information

Information may provide for:

- Development of incident objectives and Incident Action Plan (IAP)
- Identification of safety hazards
- Determination of resource needs
- Formulation of public information messages
- Analysis of incident cost



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.15

Key Points

Shared information is vital to the Incident Commander, Unified Command, and decisionmakers within supporting agencies and organizations. A single piece of information may provide input for development of incident objectives and the Incident Action Plan (IAP), identification of safety hazards, determination of resource needs, formulation of public information messages, and analysis of incident cost.

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

- **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).
- **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.

- **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.

Communications and Data Standards

Standards may include:

- A standard set of organizational structures and responsibilities.
- Common “typing” of communications resources.
- Use of agreed-upon communications protocols.
- Common identifier “titles” for personnel, facilities, and operational locations.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.16

Key Points

Communications and data standards are established to allow diverse organizations to work together effectively. Standards may include:

- A standard set of organizational structures and responsibilities.
- Common “typing” of communications resources to reflect specific capabilities.
- Use of agreed-upon communications protocols.
- Common identifier “titles” for personnel, facilities, and operational locations used to support incident operations.

Plain Language & Common Terminology



Plain language:

- Is a matter of safety.
- Facilitates interoperability across agencies/organizations, jurisdictions, and disciplines.
- Ensures that information dissemination is timely, clear, acknowledged, and understood by all intended recipients.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.17

Key Points

The **use of plain language** in emergency management and incident response:

- Is a matter of safety.
- Facilitates interoperability across agencies/organizations, jurisdictions, and disciplines.
- 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.

When necessary, information may need to be encrypted 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 protocols for using specialized encryption and tactical language should be incorporated into the Incident Action Plan or incident management communications plan

Knowledge Review and Summary

Instructions:

- Answer the review questions on the next page in your Student Manual.
- Be prepared to share your answers with the class in 5 minutes.
- If you need clarification on any of the material presented in this unit, be sure to ask your instructors.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.19

Key Points

Instructions:

- Answer the review questions on the next page.
- Be prepared to share your answers with the class in 5 minutes.
- If you need clarification on any of the material presented in this unit, ask your instructors.

Unit 4: Knowledge Review

1. What is “an overview of an incident by all relevant parties that provides incident information enabling the Incident Commander/Unified Command and any supporting agencies and organizations to make effective, consistent, and timely decisions”?

2. Match the term on the left by writing in the letter with the correct matching definition on the right.

| | Term | Description |
|-------|-------------|--|
| _____ | Reliability | A. Communication systems have been designed with sufficient expandable capacity for routine responses as well as more major incidents. |
| _____ | Portability | B. Physical protections have been installed to secure a computer network and communications equipment. |
| _____ | Scalability | C. Exercises are conducted to test that systems are able to function in any type of incident, regardless of cause, size, location, or complexity. |
| _____ | Resiliency | D. Backup power systems have been installed to maintain communications systems. Alternate communications devices, such as satellite phones, are available if standard capabilities suffer damage. |
| _____ | Redundancy | E. All equipment acquired complies with standardized radio technologies, protocols, and frequencies to ensure that it will operate at different locations and integrate seamless with other systems. |

3. What is interoperability? Why is it important?

4. Use the space below to make note of any questions you have about the material covered in this unit.

Preparedness Self-Assessment



Instructions:

- Turn to the self-assessment in your Student Manual.
- Take a few moments to complete the checklist about your organization's communications and information management systems.
- Use this information later to help strengthen your organization's response capabilities.



FEMA

NIMS Communications and Information Management
IS-0700.A – October 2014
Visual 4.20

Key Points

Instructions:

- Turn to the self-assessments in your Student Manual.
- Take a few moments to complete the checklists about your organization's communications and information management systems.
- Use this information later to help strengthen your organization's response capabilities.

Self-Assessment: Communications and Information Management Preparedness

Purpose: A common operating picture is established and maintained by the gathering, collating, synthesizing, and disseminating of incident information to all appropriate parties involved in an incident.

Instructions: Complete the following self-assessment to assess your jurisdiction's, agency's, or organization's communications and information management systems preparedness. Use this information to ensure that your jurisdiction, agency, or organization is preparing effectively.

| Communications and Information Management Systems | Yes | No |
|--|--------------------------|--------------------------|
| Comply with applicable national standards and are designed to be reliable, portable, scalable, resilient, and redundant. | <input type="checkbox"/> | <input type="checkbox"/> |
| Allow on-scene and off-scene personnel to have the same information about the incident, including the availability and location of resources and personnel, and the status of requests for assistance. | <input type="checkbox"/> | <input type="checkbox"/> |
| Specify information that will flow among all stakeholders (including the private sector, critical infrastructure owners and operators, and nongovernmental organizations). | <input type="checkbox"/> | <input type="checkbox"/> |
| Set policies and procedures for coordination and release of information to the public and media. | <input type="checkbox"/> | <input type="checkbox"/> |
| Designate the communications systems and platforms that will be used (including technical parameters of all equipment and systems). | <input type="checkbox"/> | <input type="checkbox"/> |
| Establish protocols for communications that require the use of plain language (and identify exceptions when specialized encryption and tactical language may be used). | <input type="checkbox"/> | <input type="checkbox"/> |
| Identify procedures and protocols needed to ensure operational and information security. | <input type="checkbox"/> | <input type="checkbox"/> |
| Specify interoperability and information-sharing arrangements in mutual aid agreements and assistance agreements. | <input type="checkbox"/> | <input type="checkbox"/> |
| Include periodic training and exercises to ensure that personnel capabilities and limitations of communications plans and systems are addressed before an incident. | <input type="checkbox"/> | <input type="checkbox"/> |

Use the space below to make note of action items for your jurisdiction, agency, or organization.

Your Notes: