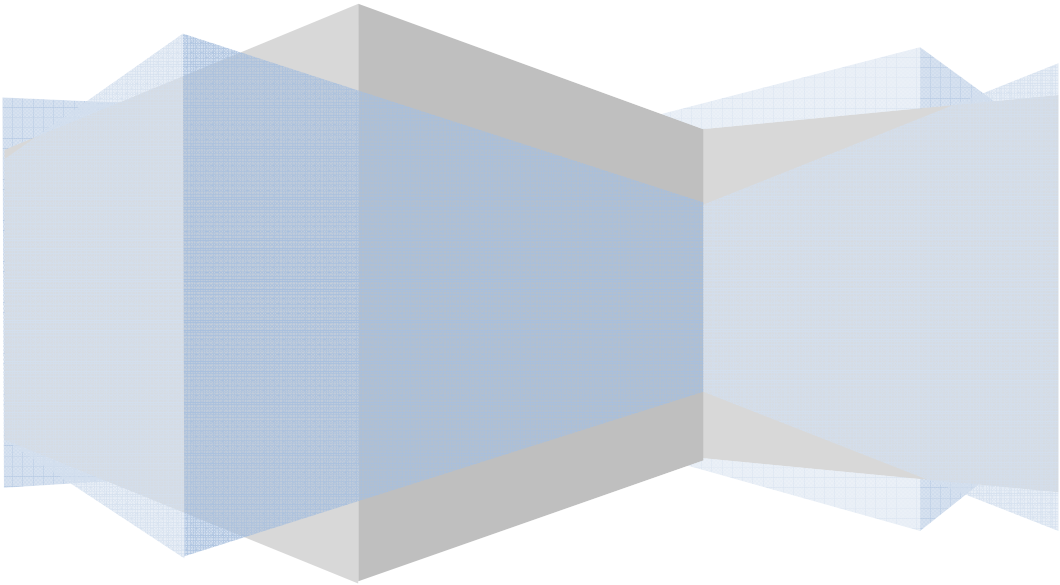
REPUBLIKA E KOSOVËS/REPUBLIKA KOSOVA/REPUBLIC OF KOSOVO

QEVERIA/VLADA/GOVERNMENT

Integrated Emergency Managment System



Pristina

Maj 2010

Acronyms:

DOC	Department Operations Centers
EMI	Emergency Management Institute
EOC	Emergency Operations Center
IEMS	Integrated Emergency Management System
IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IMT	Incident Management Teams
JIC	Joint Information Center
JIS	Joint Information System
KCPSED	Kosovo Center for Public Security, Education and Development
MACS	Multiagency Coordination System
NGOs	Nongovernmental organizations
NRP	National Response Plan
SOP	Standard operating procedures
UC	Unified Commander

Nowadays more than ever we see the need to establish an institutional coordinated system with all available resources and capacities planned for an immediate response in cases of natural disaster and other incidents. With the document presented today we make possible for the entire governmental mechanism to act in a proactive and systematic way to prevent, protect, react and rebuilt from these disasters and other incidents, in order to lessen the damage caused to human being and other socio-economic factors.

Is it about time for us to work in a more comprehensive way to coordinate our efforts in managing our response against emergency situations including natural disasters, high risk incidents, terrorism and other related incidents caused by human being. We believe that the achievement of our goals to establish this coordination mechanism and it's effectiveness is made possible through an intergovernmental cooperation, NGO sector, civil society and private sector involvement. We trust that the latter in cooperating with governmental institutions will offer enough administrative and technical as well as educational support to accelerate all possible resources to develop further policies for better response in those emergency cases in order to better serve Kosovo citizens.

The integrated system of managing emergencies offers a strategic plan to increase instituion's responsibilities, dedication and better coordination of services among stakeholders involved before and after the incidents.

In other words this system offers a systematic approach towards better guidance and preparation of all relevant agencies and departments at all levels of governance, and other nongovernmental institutions to serve Kosovo citizens at their best in cases of such emergencies, no matter it's complexity, scope, venue or cause.

Incidents and natural disasters know no boundaries. The implementation of this system offers a coordinated solution of communication and advanced field exercise at state level. Additionally this system will lead to a better regional and international cooperation which will also make the Republic of Kosovo part of these regional and international initiatives.

We trust that this integrated mechanism of managing emergencies, will be effectively implemented by all governmental agencies, at all levels, in the months to come.

Prime Minister of Kosova

Pristina, May 2010

CONTENTS

PPREFACE

On April 22, 2010, the Prime Minister of the Republic of Kosova issued Order No. 685/10 which directed the Deputy Minister of Internal Affairs to develop an *Integrated Emergency Management System* (IEMS). This system provides a consistent nationwide template to enable governments at all levels, nongovernmental organizations (NGOs), and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or their complexity. This consistency provides the foundation for utilization of IEMS for all incidents, ranging from daily occurrences to incidents requiring a coordinated Government response.

IEMS represents a core set of doctrines, concepts, principles, terminology, and organizational processes that enables effective, efficient, and collaborative incident management.

Order No. 685/10 also required the Deputy Minister of Ministry of Internal affairs to develop the *National Response Plan* (NRP). The NRP is a guide to how the State conducts all-hazards response. The NRP identifies the key principles, as well as the roles and structures that organize national response. In addition, it describes special circumstances where the Central Government exercises a larger role, including incidents where State interests are involved and catastrophic incidents where a regional and local level would require significant support.

Order No. 685/10 requires all central institutions to adopt IEMS and to use it in their individual incident management programs and activities, as well as in support of all actions taken to assist local level of government. The order requires central institutions to make adoption of IEMS by regional and local organizations a condition for central preparedness assistance IEMS recognizes the role that NGOs and the private sector have in preparedness and activities to prevent, protect against, respond to, recover from, and mitigate the effects of incidents.

Building on the foundation provided by existing emergency management and incident response systems used by jurisdictions, organizations, and functional disciplines at all levels, IEMS integrates best practices into a comprehensive framework for use nationwide by emergency management/response personnel[1] in an all-hazards context. These best practices lay the groundwork for the components of IEMS and provide the mechanisms for the further development and refinement of supporting national standards, guidelines, protocols, systems, and technologies. IEMS fosters the development of specialized technologies that facilitate emergency management and incident response activities, and allows for the adoption of new approaches that will enable continuous refinement of the system over time.

The Minister of Internal Affairs, through the Division (to be established in KCPSED) of Incident Management Systems Integration publishes the standards, guidelines, and compliance protocols for determining whether a central institutions has implemented IEMS.

Additionally, the Minister, through the KCPSED, will manages publication and collaboratively, with other institution, will develop standards, guidelines, compliance procedures, and protocols for all aspects of IEMS.

This document is developed through a collaborative intergovernmental partnership with significant input from the incident management functional disciplines, NGOs, and the private sector.

INTRODUCTION AND OVERVIEW

A. INTRODUCTION

Floods of 2005, fires in 2007 and the incident with disulfic oil in 2008 highlighted the need to focus on improving emergency management, incident response capabilities, and coordination processes across the country. A comprehensive national approach, applicable at all jurisdictional levels and across functional disciplines, improves the effectiveness of emergency management/response personnel across the full spectrum of potential incidents and hazard scenarios, including but not limited to natural hazards, terrorist activities, and other manmade disasters. Such an approach improves coordination and cooperation between public and private agencies/organizations in a variety of emergency management and incident response activities. The *Integrated Incident Management System* (IEMS) framework sets forth the comprehensive national approach (see Table 1).

Incidents typically begin and end locally, and are managed on a daily basis at the lowest possible geographical, organizational, and jurisdictional level. However, there are instances in which successful incident management operations depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines. These instances require effective and efficient coordination across this broad spectrum of organizations and activities.

IEMS uses a systematic approach to integrate the best existing processes and methods into a unified national framework for incident management. Incident management refers to how incidents are managed across all national security activities, including prevention, protection, and response, mitigation, and recovery.

This framework forms the basis for interoperability and compatibility that will, in turn, enable a diverse set of public and private organizations to conduct well-integrated and effective emergency management and incident response operations. Emergency management is the coordination and integration of all activities necessary to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, or mitigate against threatened or actual natural disasters, acts of terrorism, or other manmade disasters. It does this through a core set of concepts, principles, procedures, organizational processes, terminology, and standard requirements applicable to a broad community of IEMS users.

LEGISLATIVE FRAMEWORK

The Rpublic of Kosovo has a wide legjislative ground in the field of Emergency Menagment.

Anex. I

INSTITUTIONAL MECHANISM

All the Institutions of the Republic of Kosovo on the central and local are responsable to implement the Integrated Emergency Menagment System. The leading working group for IEMS was established from Ministry of Internal Affairs, Kosovo Security Force, Ministry of Health, Ministry of Transport and Post-Telecomunications, Situations Center, The National Security Secretariat and internationl organisations.

What is the Integrated Emergency Management System?

The *Integrated Emergency Management System* (IEMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect, respond, recover, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. IEMS works hand in hand with the *National Response Plan* (NRP). IEMS provides the template for the management of incidents, while the NRP provides the structure and mechanisms for national-level policy for incident management.

Table 1. Overview of IEMS

What IEMS Is:	What IEMS Is NOT:
▪ A comprehensive, nationwide, systematic approach to incident management, including the Incident Command System, Multiagency Coordination Systems, and Public Information • A set of preparedness concepts and principles for all hazards • Essential principles for a common operating picture and interoperability of communications and information management • Standardized resource management procedures that enable coordination among different jurisdictions or organizations	▪ A response plan ▪ Only used during large-scale incidents ▪ A communications plan ▪ Only applicable to certain emergency management/incident response personnel ▪ Only the Incident Command System or an organization chart ▪ A static system

• Scalable, so it may be used for all incidents (from day-to-day to large-scale) • A dynamic system that promotes ongoing management and maintenance	

B. CONCEPTS AND PRINCIPLES

IEMS is based on the premise that utilization of a common incident management framework will give emergency management/response personnel a flexible but standardized system for emergency management and incident response activities. IEMS is flexible because the system components can be utilized to develop plans, processes, procedures, agreements, and roles for all types of incidents; it is applicable to any incident regardless of cause, size, location, or complexity. Additionally, IEMS provides an organized set of standardized operational structures, which is critical in allowing disparate organizations and agencies to work together in a predictable, coordinated manner.

1. FLEXIBILITY

The components of IEMS are adaptable to any situation, from routine, local incidents to incidents requiring the activation of interstate mutual aid to those requiring a coordinated Governmental response, whether planned, notice or no-notice. This flexibility is essential for IEMS to be applicable across the full spectrum of potential incidents, including those that require multiagency, multijurisdictional (such as incidents that occur along international Borders), and/or multidisciplinary coordination. Flexibility in the IEMS framework facilitates scalability of emergency management and incident response activities.

2. STANDARDIZATION

Flexibility to manage incidents of any size requires coordination and standardization among emergency management/response personnel and their affiliated organizations. IEMS provides a set of standardized organizational structures that improve integration and connectivity among jurisdictions and disciplines, starting with a common foundation of preparedness and planning. Personnel and organizations that have adopted the common IEMS framework are able to work together, thereby fostering cohesion among the various organizations involved in all aspects of an incident. IEMS also provides and promotes common terminology, which fosters more effective communication among agencies and organizations responding together to an incident.

C. OVERVIEW OF IEMS COMPONENTS

IEMS integrates existing best practices into a consistent, nationwide, systematic approach to incident management that is applicable at all levels of government, nongovernmental organizations (NGOs), and the private sector, and across functional disciplines in an all-hazards context. Five major components make up this systems approach: Preparedness, Communications and Information Management, Resource Management, Command and Management, and Ongoing Management and Maintenance.

1. IEMS COMPONENTS

The components of IEMS were not designed to stand alone, but to work together in a flexible, systematic manner to provide the national framework for incident management. A more detailed discussion of each component is included in subsequent sections of this document.

a. Preparedness

Effective emergency management and incident response activities begin with a host of preparedness activities conducted on an ongoing basis, in advance of any potential incident. Preparedness involves an integrated combination of assessment; planning; procedures and protocols; training and exercises; personnel qualifications, licensure, and certification; equipment certification; and evaluation and revision.

b. Communications and Information Management

Emergency management and incident response activities rely on communications and information systems that provide a common operating picture to all command and coordination sites. IEMS describes the requirements necessary for a standardized framework for communications and emphasizes the need for a common operating picture. This component is based on the concepts of interoperability, reliability, scalability, and portability, as well as the resiliency and redundancy of communications and information systems.

c. Resource Management

Resources (such as personnel, equipment, or supplies) are needed to support critical incident objectives. The flow of resources must be fluid and adaptable to the requirements of the incident. IEMS defines standardized mechanisms and establishes the resource management process to identify requirements, order and acquire, mobilize, track and report, recover and demobilize, reimburse, and inventory resources.

d. Command and Management

The Command and Management component of IEMS is designed to enable effective and efficient incident management and coordination by providing a flexible, standardized incident management structure. The structure is based on three key organizational constructs: the Incident Command System, Multiagency Coordination Systems, and Public Information.

e. Ongoing Management and Maintenance

Within the auspices of Ongoing Management and Maintenance, there are two components: the Emergency Management Institute and Supporting Technologies.

(1) Emergency Management Institute

In order to provide a mechanism for ensuring ongoing management and maintenance of IEMS, the Ministry of Internal Affairs will establish an Emergency Management Institute in the Emergency Pillar or KPSEDC. The EMI will provide strategic direction, oversight, and coordination of IEMS and will support both routine maintenance and the continuous refinement of IEMS and its components. The EMI will oversee the program and will coordinate with central, regional and local partners in the development of compliance criteria and implementation activities. It provides guidance and support to jurisdictions and emergency management/response personnel and their affiliated organizations as they adopt or, consistent with their status, are encouraged to adopt the system. The EMI also will oversee and coordinate the publication of IEMS and its related products. This oversight includes the review and certification of training courses and exercise information.

(2) Supporting Technologies

As IEMS and its related emergency management and incident response systems will evolve, emergency management/response personnel will increasingly rely on technology and systems to implement and continuously refine IEMS. The EMI, in partnership with the science and technology section, will oversee and coordinate the ongoing development of incident management-related technology, including strategic research and development.

COMPONENT I:

PREPAREDNESS

IEMS provides the mechanisms for emergency management/response personnel[3] and their affiliated organizations to work collectively by offering the tools to enhance preparedness. Preparedness is achieved and maintained through a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action. Ongoing preparedness efforts among all those involved in emergency management and incident response activities ensure coordination during times of crisis. Moreover, preparedness facilitates efficient and effective emergency management and incident response activities.

This component describes specific measures and capabilities that emergency management/response personnel and their affiliated organizations should develop and incorporate into their overall preparedness programs to enhance the operational preparedness necessary for all-hazards emergency management and incident response activities. In developing, refining, and expanding preparedness programs and activities within their jurisdictions and/or organizations, emergency management/response personnel should leverage existing preparedness efforts and collaborative relationships to the greatest extent possible. Personal preparedness, while an important element of public security, is distinct from the operational preparedness of our country's emergency management and incident response capabilities and is beyond the scope of IEMS.

A. CONCEPTS AND PRINCIPLES

Within IEMS, preparedness focuses on the following elements: planning; procedures and protocols; training and exercises; personnel qualifications, licensure, and certification; and equipment certification. Effective adoption, implementation, and training of all IEMS components in advance of an incident or planned event will facilitate collaborative emergency management and incident response activities. Preparedness is a foundational step in emergency management and incident response; therefore, the concepts and principles that form the basis for preparedness are an integration of the concepts and principles of all IEMS components.

1. UNIFIED APPROACH

Preparedness requires a unified approach to emergency management and incident response activities. To achieve this, components of IEMS should be integrated within a jurisdiction's or organization's emergency management and incident response structure. Specifically, preparedness should be integrated into communications and information management, resource management, and command and management to form an effective system. Additionally, the unified-approach concept is at the core of the Command and Management component, as it is based on chain of command, unity of command, unity of effort, and when implemented, Unified Command. These characteristics allow organizations with different jurisdictional, geographical, or functional responsibilities, authorities, and resources to coordinate, plan, and interact effectively in support of a commonly recognized objective.

2. LEVELS OF CAPABILITY (CAPACITIES)

Preparedness involves actions to establish and sustain necessary capabilities to execute a full range of emergency management and incident response activities. For IEMS to function effectively, jurisdictions and organizations should set expectations about the capabilities and resources that will be provided before, during, and after an incident. The inventorying and categorizing of resources available for an incident or planned event is a critical element of preparedness, as it helps to establish and verify the level of capability needed.

B. ACHIEVING PREPAREDNESS (READINESS)

Individual jurisdictions should prepare in advance of an incident, in coordination with and supported by central institutions partners, NGOs, and the private sector, as appropriate. In order for successful emergency management and incident response to occur, emergency management/response personnel and their affiliated organizations must have a clear understanding of their roles and responsibilities. This clarity is essential not only for emergency management/response personnel, but also for those acting in a policy, coordination, or support role.

- ***Policy Role:*** Development, revision, signing, and/or formalization of policies, procedures, mutual aid agreements, and assistance agreements and/or plans relating to emergency management and incident response programs and activities.

- ***Coordination Role:*** Resource management or any other necessary coordination efforts required for emergency management and incident response programs and activities.

- ***Support Role:*** Provision of assistance for emergency management and incident response programs and activities.

1. IEMS AND ITS RELATIONSHIP TO THE NATIONAL RESPONSE PLAN

IEMS provides the template for the management of incidents, regardless of cause, size, location, or complexity. This template establishes the structure, concepts, principles, processes, and language for the effective employment of capabilities nationally, whether those capabilities reside with central, regional or local jurisdictions or with the private sector or NGOs.

The *National Response Plan* (NRP) is an all-hazards framework that builds upon IEMS and describes additional specific government roles and structures for incidents in which government resources are involved.

The NRP provides the structure and mechanisms for national-level policy and operational direction for incident management to ensure timely and effective central support to regional and local level related activities. The NRP is applicable to all central institutions that participate in operations requiring a coordinated central response.

IEMS and the NRP are designed to improve the incident management capabilities and overall efficiency. During incidents requiring coordinated central support, the NRP provides the guidelines and procedures to integrate capabilities and resources into a cohesive, coordinated, and seamless national framework for incident management.

A basic premise of both IEMS and the NRP is that incidents typically be managed at the local level first. In the vast majority of incidents, local resources and local mutual aid agreements and assistance agreements will provide the first line of emergency management and incident response. If additional or specialized resources or capabilities are needed, appropriate authorities may request central assistance; however, IEMS is based on the concept that local jurisdictions retain command, control, and authority over response activities for their jurisdictional areas. Adhering to IEMS allows local agencies to better utilize incoming resources.

The fundamental role of preparedness in emergency management and incident response is a universal concept incorporated in both IEMS and the NRP. Though the specific elements of preparedness described within each document may vary slightly, the concepts remain complementary. The key elements found within the Preparedness component of IEMS and the NRP are described and organized in a method to best assist stakeholders in the development of efficient, effective emergency management and incident response capabilities.

2. PREPAREDNESS ROLES

Preparedness activities should be coordinated among all appropriate agencies and organizations within the jurisdiction, as well as across jurisdictions. NGOs and the private sector should be involved in these efforts, as they often provide incident-related services, and are the owners and operators of critical infrastructure and key resources that may be involved in emergency management and incident response. Though not integrated directly into IEMS, individuals play a critical role in preparedness and are expected to prepare themselves and their families for all types of potential incidents. Jurisdictions should have programs to promote and support individual and community preparedness (e.g., public education, training sessions, demonstrations), including preparedness of those with special needs.

a. Preparedness Organizations

Preparedness organizations provide coordination for emergency management and incident response activities before an incident or planned event. These organizations range from groups of individuals to small committees to large standing organizations that represent a wide variety of committees, planning groups, or other organizations. Preparedness organizations should meet regularly and coordinate with one another to ensure an appropriate focus on helping jurisdictions and groups of jurisdictions to meet their preparedness needs.

The needs of the jurisdictions involved will dictate how frequently such organizations should conduct their business, as well as how they will be structured. When preparedness activities routinely need to be accomplished across jurisdictions, preparedness organizations should be multijurisdictional and/or multiagency and include critical infrastructure owners and operators, NGOs, and the private sector, when relevant. Memorandums or agreements should be established between necessary parties so that each will be aware of the capabilities, expectations, and roles of the others.

Preparedness organizations may take the following actions, among others:

- Establish and coordinate emergency operations plans, protocols, and procedures, including public communications and awareness.
- Integrate and coordinate the activities and functions within their purview.
- Establish the standards, guidelines, and protocols necessary to promote interoperability and consideration for responder safety.
- Adopt standards, guidelines, and procedures for requesting and providing resources.
- Identify resources and other requirements and set priorities for their use.
- Encourage training, exercises, evaluation, and corrective action programs.
- Ensure the establishment and maintenance of necessary mutual aid agreements and assistance agreements and outreach to NGOs and the private sector.
- Use Multiagency Coordination Systems, as needed and where appropriate, for planned events (such as parades or sporting events) or for specific types of incidents (such as pandemic influenza, etc.).
- Plan for operational scientific support, which can be done at each level of government, and contribute ideas to ongoing research and development of new technologies. [5]
- Conduct after-action reviews to strengthen future preparedness.

b. Elected and Appointed Officials

Elected and appointed officials should have a clear understanding of their roles and responsibilities for successful emergency management and incident response. These officials include administrative and political personnel, as well as department/agency heads who have leadership roles in a jurisdiction, including legislators and chief executives, whether elected (e.g., mayors) or appointed (e.g., regional coordinators and city managers). Although their roles may require providing direction and guidance to constituents during an incident, their day-to-day activities do not necessarily focus on emergency management and incident response.

To better serve their constituents, elected and appointed officials should do the following:

- Understand, commit to, and receive training on IEMS and participate in exercises.
- Maintain an understanding of basic emergency management, continuity of operations and continuity of government plans, jurisdictional response capabilities, and initiation of disaster declarations.
- Lead and encourage preparedness efforts within the community, agencies of the jurisdiction, NGOs, and the private sector, as appropriate.
- Help to establish relationships (including mutual aid agreements and assistance agreements) with other jurisdictions and, as appropriate, NGOs and the private sector.
- Support and encourage participation in mitigation efforts within the jurisdiction and, as appropriate, with NGOs and the private sector.
- Provide guidance to their jurisdictions, departments, and/or agencies, with clearly stated policies for IEMS implementation.
- Understand laws and regulations in their jurisdictions that pertain to emergency management and incident response.
- Maintain awareness of CIKR within their jurisdictions, potential incident impacts, and restoration priorities.

Elected and appointed officials may also be called upon to help shape and revise laws, policies, and budgets to aid in preparedness efforts and to improve emergency management and incident response activities.

An incident may have a mix of political, economic, social, environmental, public safety, public health, and financial implications with potentially serious long-term effects. Frequently, incidents require a coordinated response (across agencies, jurisdictions, and/or including NGOs and the private sector), during which elected and appointed officials must make difficult decisions under crisis conditions. Elected and appointed officials should be aware of how IEMS can work to ensure cooperative response efforts, thereby minimizing the potential implications of an incident.

(1) Elected and Appointed Officials During an Incident

Generally, elected and appointed officials are not at the scene of the incident, but should have the ability to communicate and meet with the Incident Commander (IC)/Unified Command (UC), as necessary. Depending on the nature of the incident or level of the overall emergency, elected and appointed officials could function from the following locations:

- The agency or jurisdictional offices.
- An Emergency Operations Center.
- A location housing multiagency coordination.

Elected and appointed officials should provide input on policy, direction, and authority to the IC/UC. Proper coordination between elected and appointed officials and the IC/UC can be crucial to the successful management of an incident. Elected and appointed officials should clearly communicate views to the IC/UC. As time and agency policy dictate, the following considerations should be clearly communicated, documented, and provided to the IC/UC:

- Safety considerations.
- Environmental issues.
- Legal and policy limitations.
- Issues relating to critical infrastructure services or restoration.
- Economic, political, and social concerns.
- Cost considerations.

In some circumstances, if information is not delineated in policies or laws, it should be defined through a formal delegation of authority or letter of expectation.

c. Nongovernmental Organizations

NGOs, such as community-based, faith-based, or national organizations (e.g., Red Cross), play vital roles in emergency management and incident response activities. NGOs that have the capacity and desire to be involved should be fully integrated into a jurisdiction's preparedness efforts, especially in planning, training, and exercises. Furthermore, memorandums of agreement should be established with NGOs prior to an incident so that each organization is aware of the capabilities, expectations, and roles of others.

It is recommended that key executives and administrators of NGOs use IEMS for planned events or incidents, because its use improves the organizations' ability to integrate into incident management. While compliance with IEMS is not mandated for NGOs, adhering to IEMS procedures and terminology, and requiring staff with disaster-related missions to take appropriate training, will support the continued integration of the NGOs into a jurisdiction's preparedness efforts.

d. Private Sector

The private sector plays a vital role in emergency management and incident response and should be incorporated into all aspects of IEMS. Utilities, industries, corporations, businesses, and professional and trade associations typically are involved in critical aspects of emergency response and incident management. These organizations should prepare for all-hazards incidents that may affect their ability to deliver goods and services. It is essential that private-sector organizations directly involved in emergency management and incident response, or identified as a component of critical infrastructure (e.g., hospitals, public and private utility companies, schools), be included, as appropriate, in a jurisdiction's preparedness efforts. Although private-sector entities cannot be required to be IEMS compliant, it is strongly encouraged that those private-sector organizations that are directly involved in response operations have their response personnel receive IEMS training and that the response elements of their organization be IEMS compliant.

Governments at all levels should work with the private sector to establish a common set of expectations consistent with central, regional and local roles, responsibilities, and methods of operations. These expectations should be widely disseminated and the necessary training and practical exercises conducted so that they are thoroughly understood in advance of an actual incident. These expectations are particularly important with respect to private-sector organizations involved in CIKR areas. In addition, private-sector organizations may wish to consider entering into assistance agreements with governments or other private-sector organizations to clarify the respective capabilities, roles, and expectations of the parties involved in preparing for and responding to an incident.

Finally, the private sector may be a source for best practices in emergency management and incident response.

Academia also plays a significant role in IEMS. Many academic institutions assist in providing IEMS training to responders and community leaders. Additionally, many courses of study include IEMS training and concepts in their curricula. The academic community is also a primary vehicle for the development of new concepts and principles.

4. PREPAREDNESS ELEMENTS

Preparedness efforts should validate and maintain plans, policies, and procedures, describing how they will prioritize, coordinate, manage, and support information and resources. The elements described below build the foundation necessary for efficient and effective response and recovery. Ongoing support is provided by the Emergency Management Institute (EMI) in the following areas: training and exercises; personnel qualifications, licensure, and certification; and equipment certification.

a. Preparedness Planning

Plans should be realistic, scalable, and applicable to all types of incidents, from daily occurrences to incidents requiring the activation of interstate mutual aid to those requiring a coordinated central response. Plans should form the basis of training and be exercised periodically to ensure that all individuals involved in response are able to execute their assigned tasks. It is essential that plans address training and exercising and allow for the incorporation of after-action reviews, lessons learned, and corrective actions, with responsibility agreements following any major incident or exercise. Plans should be updated periodically to reflect changes in the emergency management and incident response environment, as well as any institutional or organizational changes.

Plans should describe how personnel, equipment, and other governmental and nongovernmental resources will be used to support emergency management and incident response requirements. Plans are the operational core of preparedness and provide mechanisms for setting priorities, integrating multiple jurisdictions/organizations and functions, establishing collaborative relationships, and ensuring that communications and other systems effectively support the full spectrum of emergency management and incident response activities. Plans should also incorporate strategies for maintaining continuity of government and continuity of operations during and after incidents provide mechanisms to ensure resiliency of critical infrastructure and economic stability of communities, and incorporate the advance planning associated with responder protection, resource management, and communications and information management.

Plans should integrate all relevant departments, agencies, and organizations (including NGOs and the private sector, where appropriate) to facilitate coordinated emergency management and incident response activities. Where appropriate, plans should incorporate a clearly defined process for seeking and requesting assistance from necessary departments, agencies, or organizations. While it is recognized that jurisdictions and organizations will develop multiple types of plans, such as response, mitigation, and recovery plans, it is essential that these plans be coordinated and complement one another.

Each jurisdiction, in coordination with appropriate agencies and organizations, should develop plans that define the scope of necessary activities for preparedness, emergency management, and incident response for that jurisdiction. As appropriate, jurisdictions should also develop scenario-specific plans or annexes derived from their threat assessment. These plans should describe organizational structures, roles and responsibilities, policies, and protocols for providing support; should be flexible enough for use in all incidents; and should be comprehensive enough to meet the wide variety of public needs that may arise. While preparedness of the public is generally beyond the scope of IEMS, plans should also include public awareness, education, and communications plans and protocols.

(1) Continuity Capability

Recent natural and manmade disasters have demonstrated the need for a robust continuity capability at the central, regional and local levels, as well as within the private sector, in order to ensure the preservation of our form of government under the Constitution and the continuation of essential functions under all conditions. Ensuring that the right leadership, support staff, communications, facilities, infrastructure, and other resources with the right continuity planning and program management are available to support a jurisdiction is critical to the success of emergency management and incident response operations.

The goal of a robust continuity capability is to have the resiliency to confront any challenge, threat, or vulnerability. Continuity planning should be instituted within all organizations, include all levels of government and the private sector, and especially within those organizations that support the national essential functions.

(2) Mutual Aid Agreements and Assistance Agreements

Mutual aid agreements and assistance agreements are agreements between agencies, organizations, and jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and after an incident. A signed agreement does not obligate the provision or receipt of aid, but rather provides a tool for use should the incident dictate a need. There are several types of these kinds of agreements, including but not limited to the following:

- ***Automatic Mutual Aid:*** Agreements that permit the automatic dispatch and response of requested resources without incident-specific approvals. These agreements are usually basic contracts.

- ***Local Mutual Aid:*** Agreements between neighboring jurisdictions or organizations that involve a formal request for assistance and generally cover a larger geographic area than automatic mutual aid.
- ***Regional Mutual Aid:*** Substate regional mutual aid agreements between multiple jurisdictions that are often sponsored by a council of municipalities or a similar body.
- ***Interstate Agreements:*** Out-of-State assistance through the memorandums of understanding that supports the response effort.
- ***International Agreements:*** Agreements between the Republic of Kosova and other nations for the exchange of Central assets in an emergency.
- ***Other Agreements:*** Any agreement, whether formal or informal, used to request or provide assistance and/or resources among jurisdictions at any level of government, NGOs, or the private sector.

Jurisdictions should be party to agreements with the appropriate jurisdictions and/or organizations from which they expect to receive, or to which they expect to provide, assistance. States should participate in interstate compacts and look to establish intrastate agreements that encompass all local jurisdictions. Authorized officials from each of the participating jurisdictions and/or organizations should collectively approve all mutual aid agreements and assistance agreements.

Memorandums of understanding and memorandums of agreement are needed with the private sector and NGOs, including community-based, faith-based, and national organizations such as the Red Cross and humanitarian associations, to facilitate the timely delivery of assistance during incidents.

b. Procedures and Protocols

Procedures and protocols should detail the specific actions to implement a plan or system. All emergency management/response personnel and their affiliated organizations should develop procedures and protocols that translate into specific, action-oriented checklists for use during incident response operations.

Procedures are documented and implemented with checklists; resource listings; maps, charts, and other pertinent data; mechanisms for notifying staff; processes for obtaining and using equipment, supplies, and vehicles; methods of obtaining mutual aid agreements and assistance agreements; mechanisms for reporting information to Department Operations Centers and Emergency Operations Centers; and communications operating instructions, including connectivity among governments, NGOs, and the private sector. There are four standard levels of procedural documents:

- ***Standard Operating Procedure or Operations Manual:*** Complete reference document that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.
- ***Field Operations Guide or Incident Management Handbook:*** Durable pocket or desk guide that contains essential information required to perform specific assignments or functions.

- ***Mobilization Guide:*** Reference document used by agencies/organizations outlining agreements, processes, and procedures used by all participating organizations for activating, assembling, and transporting resources.
- ***Job Aid:*** Checklist or other visual aid intended to ensure that specific steps for completing a task or assignment are accomplished. Job aids serve as training aids to teach individuals how to complete specific job tasks.

Protocols are sets of established guidelines for actions (which may be designated by individuals, teams, functions, or capabilities) under various specified conditions. Establishing protocols provides for the standing orders, authorizations, and delegations necessary to permit the rapid execution of a task, function, or a number of interrelated functions without having to seek permission. Protocols permit specific personnel (based on training and delegation of authority) to assess a situation, take immediate steps to intervene, and escalate their efforts to a specific level before further guidance or authorizations are required.

c. Training and Exercises

Personnel with roles in emergency management and incident response at all levels of government (including persons with leadership positions, such as elected and appointed officials) should be appropriately trained to improve all-hazards capabilities nationwide. Additionally, NGOs and private-sector entities with direct roles in response operations should be strongly encouraged to participate in IEMS training and exercises. Standardized IEMS training courses focused on the structure and operational coordination processes and systems, together with courses focused on discipline-specific and agency-specific expertise, help to ensure that emergency management/response personnel can function together effectively during an incident. Training and exercises should be specifically tailored to the responsibilities of the personnel involved in incident management. Mentoring or shadowing opportunities, to allow less experienced personnel to observe those with more experience during an actual incident, should be incorporated to enhance training and exercising. Additionally, exercises should be designed to allow personnel to simulate multiple commanding, supervisory, or leadership roles whenever possible.

IEMS training levels are dependent on the individual's, jurisdiction's, or organization's level of involvement in emergency management and incident response activities. Training should allow practitioners to:

- Use the concepts and principles of IEMS in exercises, planned events, and actual incidents.
- Become more comfortable using IEMS, including the Incident Command System.

To improve IEMS performance, emergency management/response personnel should also participate in realistic exercises—including multidisciplinary, multijurisdictional incidents, and NGO and private-sector interaction—to improve coordination and interoperability. Thorough exercising of IEMS components may be done using a single exercise or a series of exercises, each of which evaluates specific aspects of IEMS and its components. Exercises should be conducted with parties identified in strategic and operational plans (e.g., the emergency operations plan), including departments, agencies, partners in mutual aid agreements and assistance agreements, NGOs, and the private sector.

Exercises should contain a mechanism for incorporating corrective actions and lessons learned from incidents into the planning process. Exercises should also cover the following:

- All aspects of a plan, particularly the processes and procedures for activating local, intrastate, and/or interstate mutual aid agreements and assistance agreements.
- Knowledge needed to activate those agreements.

d. Personnel Qualifications and Certification

A critical element of IEMS preparedness is the use of national standards that allow for common or compatible structures for the qualification, licensure, and certification of emergency management/response personnel. Standards will help ensure that these personnel possess the minimum knowledge, skills, and experience necessary to execute incident management and emergency response activities safely and effectively. Standards typically include training, experience, credentialing, validation, and physical and medical fitness. Central, regional and local certifying agencies, and professional and private organizations with personnel involved in emergency management and incident response, are encouraged to credential those individuals in their respective disciplines or jurisdictions.

The baseline criteria for this voluntary credentialing will be established by the EMI after consultation with appropriate experts, partners, and/or recognized authoritative bodies, which will detail the standards associated with the minimum thresholds for specific emergency management positions, allowing those credentialed personnel to participate, as needed, in national-level incidents.

e. Equipment Certification

Emergency management/response personnel and their affiliated organizations rely on various types and kinds of equipment to perform essential tasks. A critical component of preparedness is the acquisition of equipment that will perform to certain in standards, including the capability to be interoperable with equipment used by other jurisdictions or participating organizations.

Associated with this is the need to have a common understanding of the abilities of distinct types of equipment, to allow for better planning before an incident and rapid scaling and flexibility in meeting the needs of an incident.

5. MITIGATION

Mitigation is an important element of emergency management and incident response. It provides a critical foundation in the effort to reduce the loss of life and property and to minimize damage to the environment from natural or manmade disasters by avoiding or lessening the impact of a disaster. Mitigation provides value to the public by creating safer communities and impeding the cycle of disaster damage, reconstruction, and repeated damage. Mitigation actions should effectively be coordinated between the IC/UC and the operator of the CIKR facilities. These activities or actions, in most cases, will have a long-term sustained effect. Risk management (the process for measuring or assessing risk and developing strategies to manage it) is an essential aspect of mitigation. Risk management strategies may include avoiding the risk (e.g., removing structures in floodplains), reducing the negative effect of the risk (e.g., hardening buildings by placing barriers around them), or accepting some or all of the consequences of a particular risk.

Examples of mitigation activities include the following:

- Ongoing public education and outreach activities designed to reduce loss of life and destruction of property.
- Complying with or exceeding floodplain management and land-use regulations.
- Enforcing stringent building codes, seismic design standards, and wind-bracing requirements for new construction, or repairing or retrofitting existing buildings.
- Supporting measures to ensure the protection and resilience of CIKR designed to ensure business continuity and the economic stability of communities.
- Acquiring damaged homes or businesses in flood-prone areas, relocating the structures, and returning the property to open space, or recreational uses.
- Identifying, utilizing, and refurbishing shelters and safe rooms to help protect people in their homes, public buildings, and schools in threatened areas.
- Implementing a vital records program at all levels of government to prevent loss of crucial documents and records.
- Intelligence sharing and linkage leading to other law enforcement activities, such as infiltration of a terrorist cell to prevent an attack.
- Periodic remapping of hazard or potential hazard zones, using geospatial techniques.
- Management of data regarding historical incidents to support strategic planning and analysis.
- Development of hazard-specific evacuation routes.

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 personnel 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 IEMS. 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), 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 decision-making 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 equipped with independent power systems to ensure their continued functionality during a power failure.

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:

- ***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 Communications:*** Emergency alerts and warnings, press conferences, etc.

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 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 central, regional 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 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.

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 decision-making 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 decision makers.

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. 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 IEMS users will be designated by the Emergency Management Institute (EMI) 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.

b. Common Terminology, Plain Language, 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) 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.

e. Internet 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.

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 to 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 EMI is responsible for facilitating the development of these standards, all levels of government, NGOs, and the

COMPONENT III:

RESOURCE MANAGEMENT

Emergency management and incident response activities require carefully managed resources (personnel, teams, facilities, equipment, and/or supplies) to meet incident needs. Utilization of the standardized resource management concepts such as typing, inventorying, organizing, and tracking will facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident. Resource management should be flexible and scalable in order to support any incident and be adaptable to changes. Efficient and effective deployment of resources requires that resource management concepts and principles be used in all phases of emergency management and incident response.

From routine, local incidents to incidents that require a coordinated Central response, resource management involves the coordination, oversight, and processes that provide timely and appropriate resources during an incident. Resources may support on-scene and command operations through the Incident Command Post (ICP) or function within the Multiagency Coordination System(s) (MACS) serving at an Emergency Operations Center (EOC) or similar site.

As incident priorities are established, needs are identified, and resources are ordered, resource management systems are used to process the resource requests. In the initial stages of an incident, most of the resources requested are addressed locally or through mutual aid agreements and/or assistance agreements. As an incident grows in size or complexity, or if it starts on a large scale, resource needs may be met by other sources. In a case of competition for critical resources, MACS may be used to prioritize and coordinate resource allocation and distribution according to resource availability, needs of other incidents, and other constraints and considerations.

A. CONCEPTS AND PRINCIPLES

1. CONCEPTS

The underlying concepts of resource management are as follows:

- ***Consistency:*** Provision of a standard method for identifying, acquiring, allocating, and tracking resources.
- ***Standardization:*** Resource classification to improve the effectiveness of mutual aid agreements or assistance agreements.
- ***Coordination:*** Facilitation and integration of resources for optimal benefit.

- ***Use:*** Incorporating available resources from all levels of government, nongovernmental organizations (NGOs), and the private sector, where appropriate, in a jurisdiction's resource management planning efforts.
- ***Information Management:*** Provisions for the thorough integration of communications and information management elements into resource management organizations, processes, technologies, and decision support.
- ***Credentialing:*** Use of criteria that ensure consistent training, licensure, and certification standards.

2. PRINCIPLES

The foundations of resource management are based on the following five interwoven principles.

a. Planning

Coordinated planning, training to common standards, and inclusive exercises provide a foundation for the interoperability and compatibility of resources throughout an incident. Jurisdictions should work together in advance of an incident to develop plans for identifying, ordering, managing, and employing resources. The planning process should include identifying resource needs based on the threats to and vulnerabilities of the jurisdiction and developing alternative strategies to obtain the needed resources.

Planning may include the creation of new policies to encourage positioning of resources near the expected incident site in response to anticipated resource needs. Plans should anticipate conditions or circumstances that may trigger a specific reaction, such as the restocking of supplies when inventories reach a predetermined minimum. Organizations and jurisdictions should continually assess the status of their resources in order to have an accurate list of resources available at any given time. Additionally, emergency Management/response personnel should be familiar with the *National Response Plan* and should be prepared to integrate and/or coordinate with central resources.

b. Use of Agreements

Agreements among all parties providing or requesting resources are necessary to enable effective and efficient resource management during incident operations. This includes developing and maintaining standing agreements and contracts for services and supplies that may be needed during an incident.

c. Categorizing Resources

Resources are organized by category, kind, and type, including size, capacity, capability, skill, and other characteristics. This makes the resource-ordering and dispatch process within and across jurisdictions, and among all levels of governments, NGOs, and the private sector, more efficient and ensures that needed resources are received.

d. Resource Identification and Ordering

The resource management process uses standardized methods to identify order, mobilize, and track the resources required to support incident management activities. Those with resource management responsibilities perform these tasks either at the request of the Incident Commander (IC) or in accordance with planning requirements. Identification and ordering of resources are intertwined. In some cases, the identification and ordering process is compressed, where an IC has determined the resources necessary for the task and specifies a resource order directly. However, in larger, more complex incidents, the IC may not be fully aware of resources available. At this point, the IC may identify needs based on incident objectives and use the resource management process to fill these needs.

e. Effective Management of Resources

Resource management involves acquisition procedures, management information, and redundant systems and protocols for ordering, mobilizing, dispatching, and demobilizing resources.

(1) Acquisition Procedures

Acquisition procedures are used to obtain resources to support operational requirements. Examples include mission tasking, contracting, drawing from existing stocks, and making small purchases. A key aspect of the inventorying process is determining whether an organization needs to warehouse specific items prior to an incident. Material resources may be acquired in advance and stockpiled or obtained “just in time” through appropriate pre-incident contracts. Those with resource management responsibilities make this decision by considering the urgency of the need, whether sufficient quantities of required items are on hand, and whether the required items can be produced quickly enough to meet demand.

Another important part of the process is managing inventories with shelf-life or special maintenance considerations. Strict reliance on stockpiling raises issues concerning shelf life and durability; however, strict reliance on “just in time” resources raises its own concerns related to timely delivery. Assets that are counted on for "just in time" need to be accurately accounted for to ensure that multiple jurisdictions or private-sector organizations are not relying solely on the same response asset, which can lead to shortages during a response. Those with resource management responsibilities should build sufficient funding into their budgets for periodic replenishments, preventive maintenance, and capital improvements. An integral part of acquisition procedures is developing methods and protocols for the handling and distribution of donated resources.

(2) Management Information Systems

These systems are used to provide decision support information to managers by collecting, updating, and processing data, and tracking resources. They enhance resource status information flow and provide real-time data in a fast-paced environment where different jurisdictions, emergency management/response personnel, and their affiliated organizations are managing different aspects of the incident and should coordinate their efforts. Examples of management information systems include resource tracking, transportation tracking, inventory management, reporting, and geographical information systems. The selection and use of systems for resource management should be based on the identification of the information needs within a jurisdiction.

(3) Redundant Information Systems

Those with resource management responsibilities should be able to identify and activate backup systems to manage resources in the event that the primary resource management information system is disrupted or unavailable. Management information systems should also have sufficiently redundant and diverse power supplies and communication capabilities. If possible, the backup storage should not be co-located, and the information should be backed up at least every 24 hours during the incident.

(4) Ordering, Mobilization, and Demobilization Protocols

Protocols are followed when requesting resources, prioritizing requests, activating and mobilizing resources to incidents, and returning resources to normal status. Preparedness organizations develop standard protocols for use within their jurisdictions. Examples include tracking systems that identify the location and status of mobilized or dispatched resources, and procedures to demobilize resources and return them to their original locations and status.

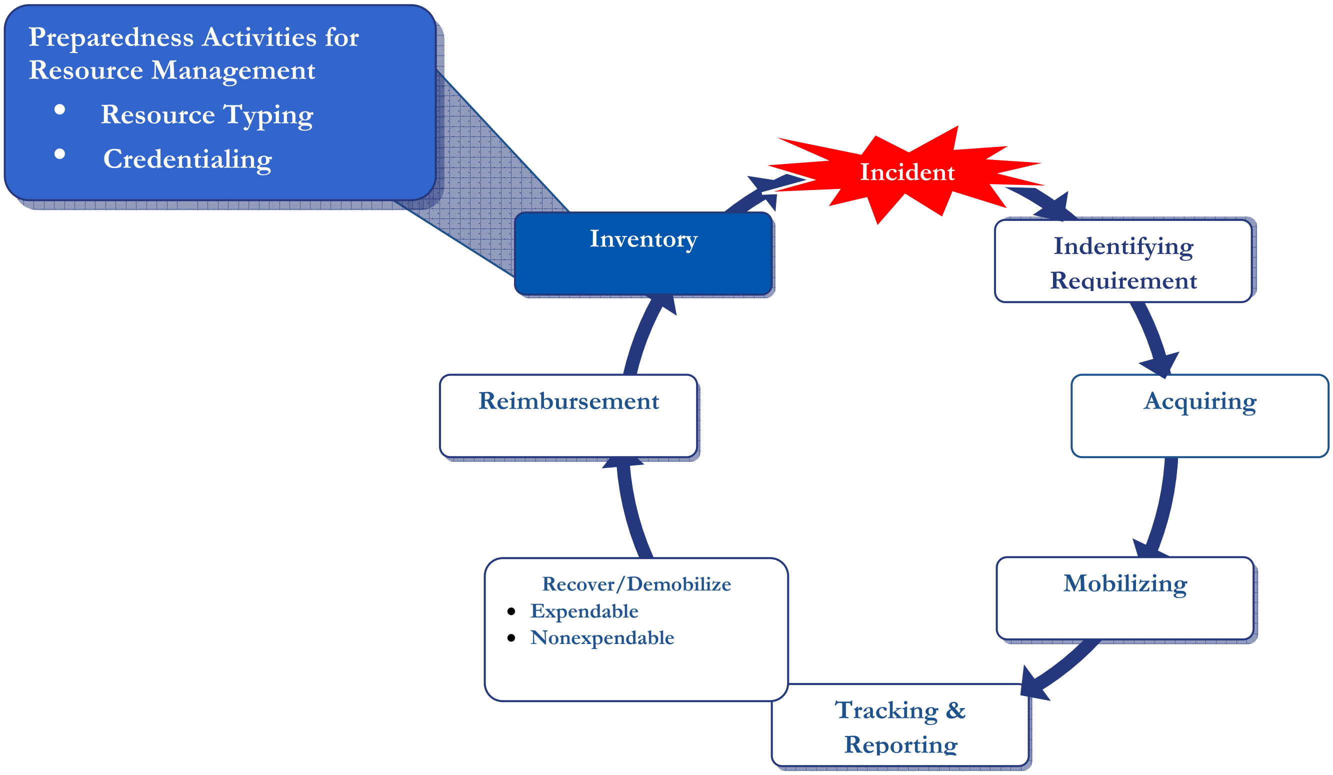
B. MANAGING RESOURCES

To implement these concepts and principles in the primary tasks of resource management, IEMS includes standardized procedures, methodologies, and functions in its seven-step resource management process. This process reflects functional considerations, geographic factors, and validated practices within and across disciplines and is continually adjusted as new lessons are learned.

Resource maintenance is important throughout all aspects of resource management. Maintenance prior to resource deployment ensures availability and capability. Maintenance during the deployment phase ensures continued capabilities, such as adequate fuel supplies during use. Post operational inspection and maintenance ensures future availability.
The foundation for resource management provided in this component will be expanded and refined over time in a collaborative cross-jurisdictional, cross-disciplinary effort led by the Emergency Management Institute (EMI).

The resource management process can be separated into two parts: resource management as an element of preparedness and resource management during an incident. The preparedness activities (resource typing, credentialing, and inventorying) are conducted on a continual basis to help ensure that resources are ready to be mobilized when called to an incident. Resource management during an incident is a finite process, as shown in Figure 1, with a distinct beginning and ending specific to the needs of the particular incident.

Figure 1 . Resource Management during an Incident



1. IDENTIFY REQUIREMENTS

When an incident occurs, those with resource management responsibilities should continually identify, refine, and validate resource requirements. This process involves accurately identifying what and how much is needed, where and when it is needed, and who will be receiving or using it. Resources to be identified in this way include equipment, supplies, facilities, and personnel or emergency response teams. If a requestor is unable to describe an item by resource type or classification, those with resource management responsibilities should provide technical advice to enable the requirements to be defined and translated into a specification.

Resource availability and requirements will constantly change as the incident evolves. Consequently, all emergency management/response personnel and their affiliated organizations participating in an operation should coordinate closely throughout this process. Coordination should begin as early as possible, preferably prior to the need for incident response activities.

In instances when an incident is projected to have catastrophic implications (e.g., a major hurricane or flooding), Government and her regional branches may position resources in the anticipated incident area. In cases where there is time to assess the requirements and plan for a catastrophic incident, the central response will be coordinated with regional and local jurisdictions, and the positioning of central resources will be tailored to address the specific situation.

2. ORDER AND ACQUIRE

Requests for resources that cannot be obtained locally are submitted using standardized resource-ordering procedures. These requests are generally forwarded first to an adjacent locality or sub-state region and then to the center.

The decision cycles for placing and filling resource orders are different for field/incident personnel with resource management responsibilities and resource coordination processes such as MACS. The IC will develop resource requests based on priorities that consider current and successive operational periods. Decisions about resource allocation are based on organization or agency protocol and possibly the resource demands of other incidents. Requested resources will be mobilized only with the consent of the jurisdiction that is being asked to provide the resources. Discrepancies between requested resources and those available for delivery must be communicated to the requestor.

3. MOBILIZE

Emergency management/response personnel begin mobilizing when notified through established channels. At the time of notification, they are given the date, time, and place of departure; mode of transportation to the incident; estimated date and time of arrival; reporting location (address, contact name, and phone number); anticipated incident assignment; anticipated duration of deployment; resource order number; incident number; and applicable cost and funding codes. The resource-tracking and mobilization processes are directly linked. When resources arrive on scene, they must be formally checked in. This starts the on-scene check-in process and validates the order requirements. Notification that the resources have arrived is made through the appropriate channels.

The mobilization process may include deployment planning based on existing interagency mobilization guidelines; equipping; training; designating assembly points that have facilities suitable for logistical support; and obtaining transportation to deliver resources to the incident most quickly, in line with priorities and budgets. Mobilization plans should also recognize that some resources are fixed facilities, such as laboratories, hospitals, EOCs, shelters, and waste management systems. These facilities assist operations without moving into the incident area in the way that other resources are mobilized. Plans and systems to monitor resource mobilization status should be flexible enough to adapt to both types of mobilization.

Managers should plan and prepare for the demobilization process at the same time that they begin the resource mobilization process. Early planning for demobilization facilitates accountability and makes the transportation of resources as efficient as possible—in terms of both costs and time of delivery.

4. TRACK AND REPORT

Resource tracking is a standardized, integrated process conducted prior to, during, and after an incident by all emergency management/response personnel and their affiliated organizations, as appropriate. This process provides a clear picture of where resources are located; helps staff prepare to receive resources; protects the safety and security of equipment, supplies, and personnel; and enables their coordination and movement. Those with resource management responsibilities use established procedures to track resources continuously from mobilization through demobilization. Managers should follow all procedures for acquiring and managing resources, including reconciliation, accounting, auditing, and inventorying.

5. RECOVER AND DEMOBILIZE

Recovery involves the final disposition of all resources, including those located at the incident site and at fixed facilities. During this process, resources are rehabilitated, replenished, disposed of, and/or retrograded.

Demobilization is the orderly, safe, and efficient return of an incident resource to its original location and status. It can begin at any point of an incident, but should begin as soon as possible to facilitate accountability. The demobilization process should coordinate between incident(s) and MACS to reassign resources, if necessary, and to prioritize critical resource needs during demobilization.

The Demobilization Unit in the Planning Section develops an Incident Demobilization Plan, containing specific demobilization instructions, as part of the Incident Action Plan. Demobilization planning and processes should include provisions addressing the safe return of resources to their original location and status, and notification of return. Demobilization should also include processes for tracking resources and for addressing applicable reimbursement. Furthermore, documentation regarding the transportation of resources should be collected and maintained for reimbursement, if applicable. Demobilization provisions may need to meet specific organizational requirements.

a. Nonexpendable Resources

Nonexpendable resources (such as personnel, fire engines, and durable equipment) are fully accounted for both during the incident and when they are returned to the providing organization. The organization then restores the resources to fully functional capability and readies them for the next mobilization. Broken or lost items should be replaced through the appropriate resupply process by the organization with invoicing responsibility for the incident, or as defined in existing agreements. It is critical that fixed-facility resources also be restored to their full functional capability in order to ensure readiness for the next mobilization. In the case of human resources, such as Incident Management Teams, adequate rest and recuperation time and facilities should be provided. Important occupational health and mental health issues should also be addressed, including monitoring the immediate and long-term effects of the incident (chronic and acute) on emergency management/response personnel.

b. Expendable Resources

Expendable resources, such as water, food, fuel, and other one-time-use supplies, must be fully accounted for. The incident management organization bears the costs of expendable resources, as authorized in financial agreements executed by preparedness organizations. Returned resources that are not in restorable condition, whether expendable or non-expendable, must be declared as excess according to established regulations and policies of the controlling jurisdiction, agency, or organization. Waste management is of special note in the process of recovering resources, as resources that require special handling and disposition (e.g., biological waste and contaminated supplies, debris, and equipment) are handled according to established regulations and policies.

6. REIMBURSE

Reimbursement provides a mechanism to recoup funds expended for incident-specific activities. Processes for reimbursement play an important role in establishing and maintaining the readiness of resources and should be in place to ensure that resource providers are reimbursed in a timely manner. They should include mechanisms for collecting bills, validating costs against the scope of the work, ensuring that proper authorities are involved, and accessing reimbursement programs. Reimbursement mechanisms should be included in preparedness plans, mutual aid agreements, and assistance agreements. Some resources rendered may or may not be reimbursed, based on agreements established before the incident.

7. INVENTORY

Resource management uses various resource inventory systems to assess the availability of assets provided by jurisdictions. Preparedness organizations should inventory and maintain current data on their available resources. The data are then made available to communications/dispatch centers and EOCs and organizations within MACS. Resources identified within an inventory system are not an indication of automatic availability. The jurisdiction and/or owner of the resources have the final determination on availability.

Inventory systems for resource management should be adaptable and scalable and should account for the potential of double-counting personnel and/or equipment. In particular, resource summaries should clearly reflect any overlap of personnel across different resource pools. Personnel inventories should reflect single resources with multiple skills, taking care not to overstate the total resources. For example, many firefighters also have credentials as emergency medical technicians (EMTs). A resource summary, then, could count a firefighter as a firefighter or as an EMT, but not as both. The total should reflect the number of available personnel, not simply the sum of the firefighter and EMT counts.

Deployable resources have different inventory, ordering, and response profiles depending on their primary use during the response or recovery phases of an incident. Planning for resource use, inventory, and tracking should recognize the fundamental difference in resource deployment in the response and recovery phases. The response phase relies heavily on mutual aid agreements and assistance agreements, while recovery resources are typically acquired through contracts with NGOs and/or the private sector.

a. Credentialing

The credentialing process entails the objective evaluation and documentation of an individual's current certification, license, or degree; training and experience; and competence or proficiency to meet nationally accepted standards, provide particular services and/or functions, or perform specific tasks under specific conditions during an incident.

For the purpose of IEMS, credentialing is the administrative process for validating personnel qualifications and providing authorization to perform specific functions and to have specific access to an incident involving mutual aid.

While credentialing includes the issuing of identification cards or credentials, it is separate and distinct from the incident badging process. When access to a site is controlled through special badging, the badging process must be based on verification of identity, qualifications, and deployment authorization.

Organizations utilizing volunteers, especially spontaneous volunteers, are responsible for ensuring each volunteer's eligibility to participate in a response. These organizations—governmental agencies responsible for coordinating emergency responses, volunteer management agencies (e.g., Red Cross), and other potential users of volunteers (e.g., hospitals, fire and police departments, etc.) must develop protocols governing the activation and use of volunteers.

b. Identifying and Typing Resources

Resource typing is categorizing, by capability, the resources requested, deployed, and used in incidents.[17] Measurable standards identifying resource capabilities and performance levels serve as the basis for categories. Resource users at all levels use these standards to identify and inventory resources. Resource kinds may be divided into subcategories to define more precisely the capabilities needed to meet specific requirements. Resource typing is a continuous process designed to be as simple as possible; it facilitates frequent use and accuracy in obtaining needed resources. To allow resources to be deployed and used on a national basis, the EMI (with input from Central, State, tribal, local, private- sector, nongovernmental, and national professional organizations) is responsible for facilitating the development and issuance of national standards for resource typing and ensuring that these typed resources reflect operational capabilities.

(1) Category

This is the function for which a resource would be most useful. Table 2 lists examples of categories used in a national resource-typing protocol.

Table 2. Example Categories for National Resource Typing

- Transportation
- Communications
- Public works and
- Health and medical
- Search and rescue
- Hazardous materials

engineering
- Firefighting
- Information and planning
- Law enforcement and security
- Mass care
- Resource management

response
- Food and water
- Energy
- Public information
- Animals and agricultural issues
- Volunteers and donations

(2) Kind

Kind refers to broad classes that characterize like resources, such as teams, personnel, equipment, supplies, vehicles, and aircraft.

(a) Components

Components are the elements that make up a resource. For example, an engine company may be listed as having the eight components shown in Table 3.

Table 3. Example of a Resource with Multiple Components (Firefighting Engine Company)

(1) Pomp
(2) Hose 2½″
(3) Hose 1¾″
(4) Hand tools
(5) Water tank
(6) Ladder
(7) Master stream
(8) Personnel

As another example, urban search and rescue teams consist of two 31-person teams, four canines, and a comprehensive equipment cache. The cache is divided into five separate color-coded elements and is stored in containers that meet specific requirements.

(b) Measures

Measures are standards that identify capability and/or capacity. The specific measures used will depend on the kind of resource being typed and the mission envisioned. Measures must be useful in describing a resource's capability to support the mission. As an example, one measure for a disaster medical assistance team is the number of patients it can care for per day. An appropriate measure for a hose might be the number of gallons of water per hour that can flow through it.

(3) Type

Type refers to the level of resource capability. Assigning the Type 1 label to a resource implies that it has a greater level of capability than a Type 2 of the same resource (for example, due to its power, size, or capacity), and so on to Type 4. Typing provides managers with additional information to aid in the selection and best use of resources. In some cases, a resource may have fewer than or more than four types; in such cases, either additional types will be identified, or the type will be described as "not applicable." The type assigned to a resource or a component is based on a minimum level of capability described by the identified measure(s) for that resource.

COMPONENT IV:

COMMAND AND MANAGEMENT

The IEMS components discussed previously (Preparedness, Communications and Information Management, and Resource Management) provide a framework to facilitate clear response authority, resource acquisition, and effective management during incident response. The Incident Command System (ICS), Multiagency Coordination System (MACS), and Public Information are the fundamental elements of incident management. These elements provide standardization through consistent terminology and established organizational structures. Emergency management and incident response refer to the broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support. Incident management, by distinction, includes directing specific incident operations; acquiring, coordinating, and delivering resources to incident sites; and sharing information about the incident with the public. Taken together, these elements of Command and Management are the most visible aspects of incident management, typically executed with a sense of urgency. This component describes the systems used to facilitate incident Command and Management operations.

A. INCIDENT COMMAND SYSTEM

Most incidents are managed locally and are typically handled by local communications/ dispatch centers and emergency management/response personnel[19] within a single jurisdiction. The majority of responses need go no further. In other instances, incidents that begin with a single response within a single jurisdiction rapidly expand to multidisciplinary, multijurisdictional levels requiring significant additional resources and operational support. ICS provides a flexible core mechanism for coordinated and collaborative incident management, whether for incidents where additional resources are required or are provided from different organizations within a single jurisdiction or outside the jurisdiction, or for complex incidents with national implications (such as an emerging infectious disease or a bioterrorism attack). When a single incident covers a large geographical area, multiple local emergency management and incident response agencies may be required. The responding "agencies" are defined as the governmental agencies, though in certain circumstances nongovernmental organizations (NGOs) and private-sector organizations may be included. Effective cross-jurisdictional coordination using processes and systems is absolutely critical in this situation.

ICS is a widely applicable management system designed to enable effective, efficient incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. ICS is a fundamental form of management established in a standard format, with the purpose of enabling incident managers to identify the key concerns associated with the incident—often under urgent conditions—without sacrificing attention to any component of the command system.

ICS is used to organize on-scene operations for a broad spectrum of emergencies from small to complex incidents, both natural and manmade. The field response level is where emergency management/response personnel, under the command of an appropriate authority, carry out tactical decisions and activities in direct response to an incident or threat. Resources from central, regional and local levels, when appropriately deployed, become part of the field ICS as prescribed by the local authority.

As a system, ICS is extremely useful; not only does it provide an organizational structure for incident management, but it also guides the process for planning, building, and adapting that structure. Using ICS for every incident or planned event helps hone and maintain skills needed for the large-scale incidents.

ICS is used by all levels of government as well as by many NGOs and the private sector. ICS is also applicable across disciplines. It is normally structured to facilitate activities in five major functional areas: Command, Operations, Planning, Logistics, and Finance/Administration. Intelligence/Investigations is an optional sixth functional area that is activated on a case-by-case basis.

Acts of biological, chemical, radiological, and nuclear terrorism may present unique challenges for the traditional ICS structure. Incidents that are not site specific, are geographically dispersed, or evolve over longer periods of time will require extraordinary coordination among all participants, including all levels of government, as well as NGOs and the private sector.

1. MANAGEMENT CHARACTERISTICS

ICS is based on 14 proven management characteristics, each of which contributes to the strength and efficiency of the overall system.

a. Common Terminology

ICS establishes common terminology that allows diverse incident management and support organizations to work together across a wide variety of incident management functions and hazard scenarios. This common terminology covers the following:

(1) Organizational Functions

Major functions and functional units with incident management responsibilities are named and defined. Terminology for the organizational elements is standard and consistent.

(2) Resource Descriptions

Major resources (including personnel, facilities, and major equipment and supply items) that support incident management activities are given common names and are "typed" with respect to their capabilities, to help avoid confusion and to enhance interoperability.

(3) Incident Facilities

Common terminology is used to designate the facilities in the vicinity of the incident area that will be used during the course of the incident.

b. Modular Organization

The ICS organizational structure develops in a modular fashion based on the size and complexity of the incident, as well as the specifics of the hazard environment created by the incident. When needed, separate functional elements can be established, each of which may be further subdivided to enhance internal organizational management and external coordination. Responsibility for the establishment and expansion of the ICS modular organization ultimately rests with Incident Command, which bases the ICS organization on the requirements of the situation. As incident complexity increases, the organization expands from the top down as functional responsibilities are delegated. Concurrently with structural expansion, the number of management and supervisory positions expands to address the requirements of the incident adequately.

c. Management by Objectives

Management by objectives is communicated throughout the entire ICS organization and includes:

- Establishing incident objectives.
- Developing strategies based on incident objectives.
- Developing and issuing assignments, plans, procedures, and protocols.

- Establishing specific, measurable tactics or tasks for various incident management functional activities, and directing efforts to accomplish them, in support of defined strategies.
- Documenting results to measure performance and facilitate corrective actions.

d. Incident Action Planning

Centralized, coordinated incident action planning should guide all response activities. An Incident Action Plan (IAP) provides a concise, coherent means of capturing and communicating the overall incident priorities, objectives, strategies, and tactics in the context of both operational and support activities.

Every incident must have an action plan. However, not all incidents require written plans. The need for written plans and attachments is based on the requirements of the incident and the decision of the Incident Commander (IC) or Unified Command (UC). Most initial response operations are not captured with a formal IAP. However, if an incident is likely to extend beyond one operational period, become more complex, or involve multiple jurisdictions and/or agencies, preparing a written IAP will become increasingly important to maintain effective, efficient, and safe operations.

e. Manageable Span of Control

Span of control is key to effective and efficient incident management. Supervisors must be able to adequately supervise and control their subordinates, as well as communicate with and manage all resources under their supervision. The type of incident, nature of the task, hazards and safety factors, and distances between personnel and resources all influence span-of-control considerations.

f. Incident Facilities and Locations

Various types of operational support facilities are established in the vicinity of an incident, depending on its size and complexity, to accomplish a variety of purposes. The IC will direct the identification and location of facilities based on the requirements of the situation. Typically designated facilities include Incident Command Posts, Bases, Camps, Staging Areas, mass casualty triage areas, point-of-distribution sites, and others as required.

g. Comprehensive Resource Management

Maintaining an accurate and up-to-date picture of resource utilization is a critical component of incident management and emergency response. Resources to be identified in this way include personnel, teams, equipment, supplies, and facilities available or potentially available for assignment or allocation. Resource management is described in detail in Component III.

h. Integrated Communications

Incident communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures. This integrated approach links the operational and support units of the various agencies, involved and is necessary to maintain communications connectivity and discipline and to enable common situational awareness and interaction. Preparedness planning should address the equipment, systems, and protocols necessary to achieve integrated voice and data communications.

i. Establishment and Transfer of Command

The command function must be clearly established from the beginning of incident operations. The agency with primary jurisdictional authority over the incident designates the individual at the scene responsible for establishing command. When command is transferred, the process must include a briefing that captures all essential information for continuing safe and effective operations.

j. Chain of Command and Unity of Command

Chain of command refers to the orderly line of authority within the ranks of the incident management organization. Unity of command means that all individuals have a designated supervisor to whom they report at the scene of the incident. These principles clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers at all levels must be able to direct the actions of all personnel under their supervision.

k. Unified Command

In incidents involving multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement, Unified Command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.

l. Accountability

Effective accountability of resources at all jurisdictional levels and within individual functional areas during incident operations is essential. To that end, Check-In/Check-Out, Incident Action Planning, Unity of Command, Personal Responsibility, Span of Control, and Resource Tracking are the principles of accountability, which must be adhered to.

m. Dispatch/Deployment

Resources should respond only when requested or when dispatched by an appropriate authority through established resource management systems. Resources not requested must refrain from spontaneous deployment to avoid overburdening the recipient and compounding accountability challenges.

n. Information and Intelligence Management

The incident management organization must establish a process for gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.

2. INCIDENT COMMAND AND COMMAND STAFF

Incident Command is responsible for overall management of the incident. Overall management includes Command Staff assignments required to support the command function. The Command and General Staffs are typically located at the Incident Command Post (ICP).

a. Incident Command

The command function may be conducted in one of two general ways:

(1) Single Incident Commander

When an incident occurs within a single jurisdiction and there is no jurisdictional or functional agency overlap, a single IC should be designated with overall incident management responsibility by the appropriate jurisdictional authority. (In some cases where incident management crosses jurisdictional and/or functional agency boundaries, a single IC may be designated if agreed upon.) Jurisdictions should consider designating ICs for established Incident Management Teams (IMTs).

The designated IC will develop the incident objectives on which subsequent incident action planning will be based. The IC will approve the IAP and all requests pertaining to ordering and releasing incident resources.

(2) Unified Command

UC is an important element in multijurisdictional or multiagency incident management. It provides guidelines to enable agencies with different legal, geographic, and functional responsibilities to coordinate, plan, and interact effectively. As a team effort, UC allows all agencies with jurisdictional authority or functional responsibility for the incident to jointly provide management direction through a common set of incident objectives and strategies and a single IAP. Each participating agency maintains its authority, responsibility, and accountability.

UC functions as a single integrated management organization, which involves:

- Co-located command at the ICP.
- One Operations Section Chief to direct tactical efforts.
- A coordinated process for resource ordering.
- Shared planning, logistical, and finance/administration functions, wherever possible.

- Coordinated approval of information releases.

All agencies in the UC structure contribute to the process of:

- Selecting objectives.
- Determining overall incident strategies.
- Ensuring that joint planning for tactical activities is accomplished in accordance with approved incident objectives.
- Ensuring the integration of tactical operations.
- Approving, committing, and making optimum use of all assigned resources.

The exact composition of the UC structure will depend on the location(s) of the incident (i.e., which geographical jurisdictions or organizations are involved) and the type of incident (i.e., which functional agencies of the involved jurisdiction(s) or organization(s) are required). The designation of a single IC for some multijurisdictional incidents, if planned for in advance, may be considered in order to promote greater unity of effort and efficiency.

The designated agency officials participating in the UC represent different legal authorities and functional areas of responsibility and use a collaborative process to establish, identify, and rank incident priorities and to determine appropriate objectives consistent with the priorities. Agencies that are involved in the incident but lack jurisdictional responsibility or authorities are defined as supporting and/or assisting agencies. They are represented in the command structure and effect coordination on behalf of their parent agency through the Liaison Officer. Jurisdictional responsibilities of multiple incident management officials are consolidated into a single planning process that includes:

- Responsibilities for incident management.
- Incident objectives.
- Resource availability and capabilities.
- Limitations.
- Areas of agreement and disagreement between agency officials.

Incidents are managed under a single collaborative approach that includes:

- Common organizational structure.
- Single Incident Command Post.
- Unified planning process.
- Unified resource management.

Under UC, the IAP is assembled by the Planning Section and is approved by the UC. A single individual, the Operations Section Chief, directs the tactical implementation of the IAP. The Operations Section Chief will usually come from the organization with the greatest jurisdictional involvement. UC participants will agree on the designation of the Operations Section Chief.

UC works best when the participating members of the UC co-locate at the ICP and observe the following practices:

- Select an Operations Section Chief for each operational period.
- Keep each other informed of specific requirements.
- Establish consolidated incident objectives, priorities, and strategies.
- Establish a single system for ordering resources.
- Develop a consolidated written or oral IAP to be evaluated and updated at regular intervals.
- Establish procedures for joint decision-making and documentation.

b. Command Staff

In an incident command organization, the Command Staff typically includes a Public Information Officer, a Safety Officer, and a Liaison Officer, who report directly to the IC/UC and may have assistants as necessary (see Figure 4). Additional positions may be required, depending on the nature, scope, complexity, and location(s) of the incident(s), or according to specific requirements established by the IC/UC.

(1) Public Information Officer

The Public Information Officer is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements. The Public Information Officer gathers, verifies, coordinates, and disseminates accurate, accessible, and timely information on the incident’s cause, size, and current situation; resources committed; and other matters of general interest for both internal and external audiences. The Public Information Officer may also perform a key public information-monitoring role. Whether the command structure is single or unified, only one Public Information Officer should be designated per incident. Assistants may be assigned from other involved agencies, departments, or organizations. The IC/UC must approve the release of all incident-related information. In large-scale incidents or where multiple command posts are established, the Public Information Officer should participate in or lead the Joint Information Center (JIC) in order to ensure consistency in the provision of information to the public.

(2) Safety Officer

The Safety Officer monitors incident operations and advises the IC/UC on all matters relating to operational safety, including the health and safety of emergency responder personnel. The ultimate responsibility for the safe conduct of incident management operations rests with the IC/UC and supervisors at all levels of incident management. The Safety Officer is, in turn, responsible to the IC/UC for the systems and procedures necessary to ensure ongoing assessment of hazardous environments, including the incident Safety Plan, coordination of multiagency safety efforts, and implementation of measures to promote emergency responder safety as well as the general safety of incident operations. The Safety Officer has immediate authority to stop and/or prevent unsafe acts during incident operations. It is important to note that the agencies, organizations, or jurisdictions that contribute to joint safety management efforts do not lose their individual identities or responsibility for their own programs, policies, and personnel. Rather, each contributes to the overall effort to protect all responder personnel involved in incident operations.

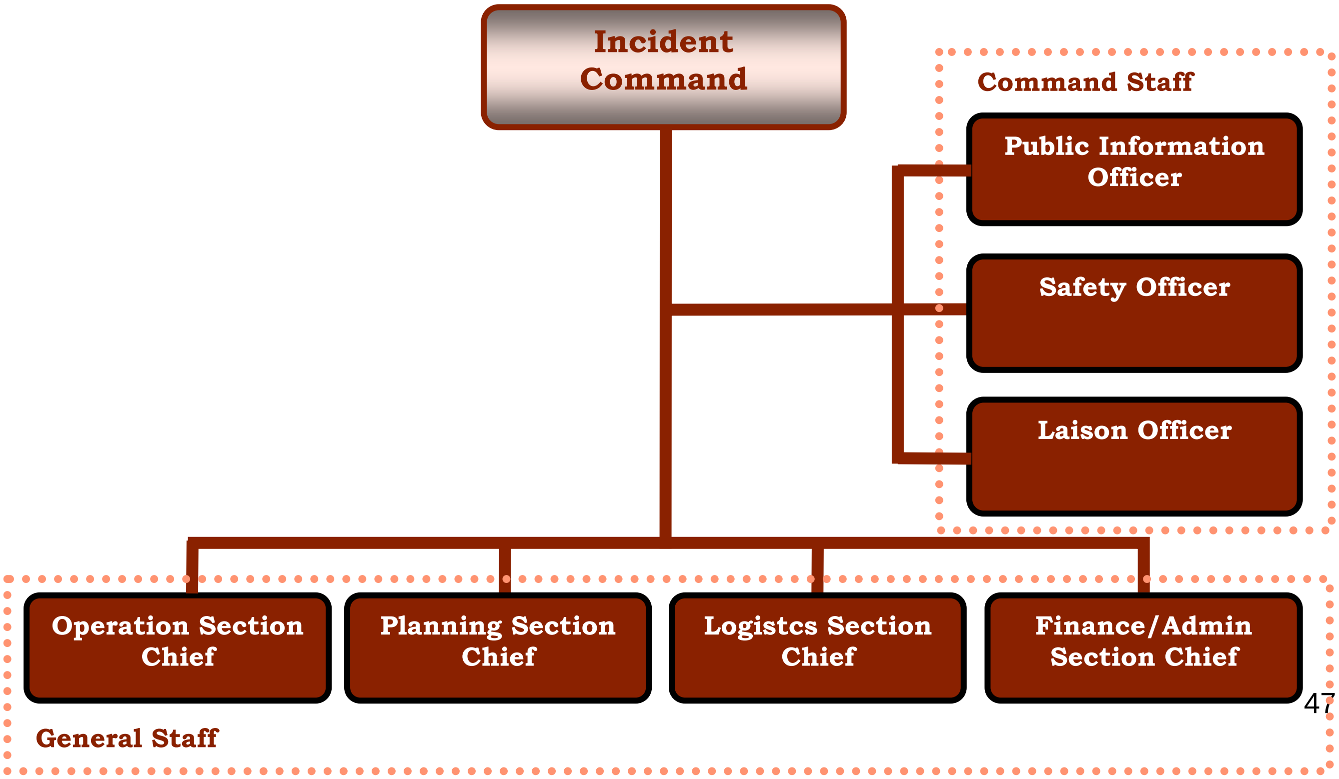
(3) Liaison Officer

The Liaison Officer is Incident Command's point of contact for representatives of other governmental agencies, NGOs, and the private sector (with no jurisdiction or legal authority) to provide input on their agency's policies, resource availability, and other incident-related matters. Under either a single-IC or a UC structure, representatives from assisting or cooperating agencies and organizations coordinate through the Liaison Officer. Agency and organizational representatives assigned to an incident must have the authority to speak for their parent agencies or organizations on all matters, following appropriate consultations with their agency leadership. Assistants and personnel from other agencies or organizations, public or private, involved in incident management activities may be assigned to the Liaison Officer to facilitate coordination.

(4) Additional Command Staff

Additional Command Staff positions may also be necessary, depending on the nature and location(s) of the incident or specific requirements established by Incident Command. For example, a legal counsel might be assigned to the Planning Section as a technical specialist or directly to the Command Staff to advise Incident Command on legal matters, such as emergency proclamations, the legality of evacuation and quarantine orders, and legal rights and restrictions pertaining to media access. Similarly, a medical advisor might be designated to provide advice and recommendations to Incident Command about medical and mental health services, mass casualty, acute care, vector control, epidemiology, or mass prophylaxis considerations, particularly in response to a bioterrorism incident. In addition, a special needs advisor might be designated to provide expertise regarding communication, transportation, supervision, and essential services for diverse populations in the affected area.

Figure 4. Incident Command System: Command Staff and General Staff



c. Incident Command Organization

The incident Command and Management organization is located at the ICP. Incident Command directs operations from the ICP, which is generally located at or in the immediate vicinity of the incident site. Typically, one ICP is established for each incident. As emergency management/response personnel deploy, they must, regardless of agency affiliation, report to and check in at the designated Staging Area, Base, Camp, or location and notify the IC/UC to receive an assignment in accordance with the procedures established by the IC/UC.

3. GENERAL STAFF

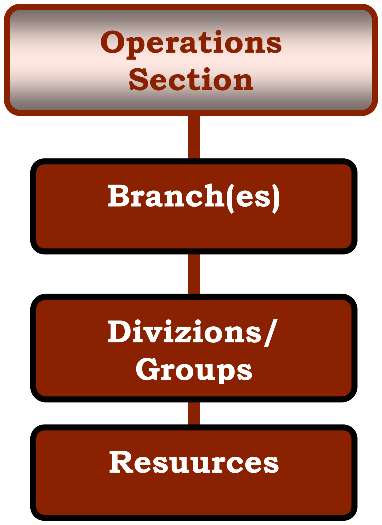
The General Staff is responsible for the functional aspects of the incident command structure. The General Staff typically consists of the Operations, Planning, Logistics, and Finance/Administration Section Chiefs. The Section Chiefs may have one or more deputies assigned, with the assignment of deputies from other agencies encouraged in the case of multijurisdictional incidents. The functional Sections are discussed more fully below.

a. Operations Section

This Section is responsible for all tactical activities focused on reducing the immediate hazard, saving lives and property, establishing situational control, and restoring normal operations. Lifesaving and responder safety will always be the highest priorities and the first objectives in the IAP.

Figure 5 depicts the organizational template for an Operations Section. Expansions of this basic structure may vary according to numerous considerations and operational factors. In some cases, a strictly functional approach may be used. In other cases, the organizational structure will be determined by geographical/jurisdictional boundaries. In still others, a mix of functional and geographical considerations may be appropriate. ICS offers flexibility in determining the right structural approach for the specific circumstances of the incident at hand.

Figure 5. Major Organisational Elements of Operations Section



(1) Operations Section Chief

The Operations Section Chief is responsible to Incident Command for the direct management of all incident-related tactical activities. The Operations Section Chief will establish tactics for the assigned operational period. An Operations Section Chief should be designated for each operational period, and responsibilities include direct involvement in development of the IAP.

(2) Branches

Branches may be functional, geographic, or both, depending on the circumstances of the incident. In general, Branches are established when the number of Divisions or Groups exceeds the recommended span of control. Branches are identified by the use of Roman numerals or by functional area.

(3) Divisions and Groups

Divisions and/or Groups are established when the number of resources exceeds the manageable span of control of Incident Command and the Operations Section Chief. Divisions are established to divide an incident into physical or geographical areas of operation. Groups are established to divide the incident into functional areas of operation. For certain types of incidents, for example, Incident Command may assign evacuation or mass-care responsibilities to a functional Group in the Operations Section. Additional levels of supervision may also exist below the Division or Group level.

(4) Resources

Resources may be organized and managed in three different ways, depending on the requirements of the incident.

- *Single Resources:* Individual personnel or equipment and any associated operators.
- *Task Forces:* Any combination of resources assembled in support of a specific mission or operational need. All resource elements within a Task Force must have common communications and a designated leader.
- *Strike Teams:* A set number of resources of the same kind and type that have an established minimum number of personnel. All resource elements within a Strike Team must have common communications and a designated leader.

The use of Task Forces and Strike Teams is encouraged, when appropriate, to optimize the use of resources, reduce the span of control over a large number of single resources, and reduce the complexity of incident management coordination and communications.

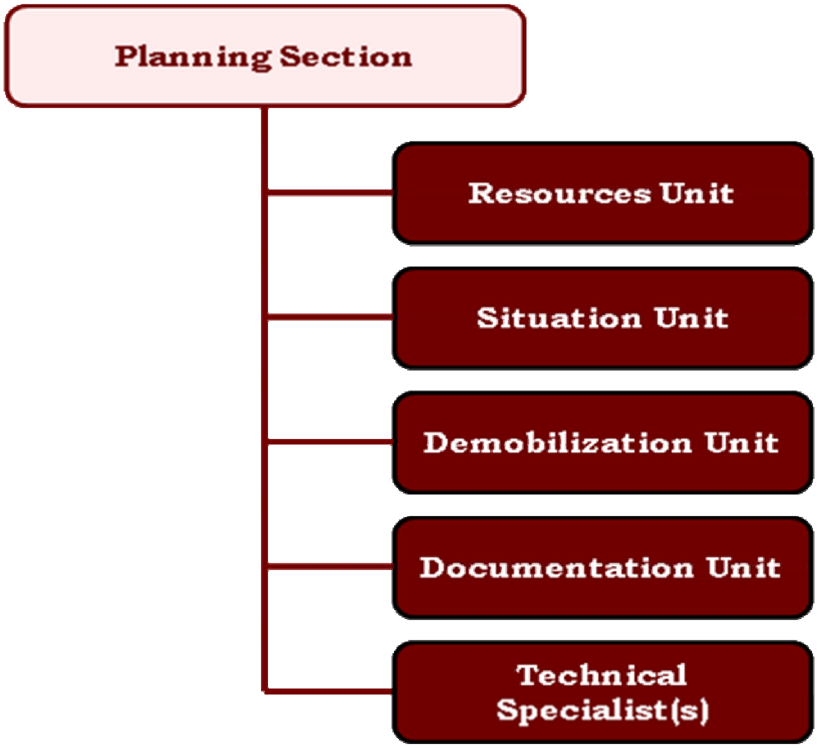
b. Planning Section

The Planning Section collects, evaluates, and disseminates incident situation information and intelligence to the IC/UC and incident management personnel. This Section then prepares status reports, displays situation information, maintains the status of resources assigned to the incident, and prepares and documents the IAP, based on Operations Section input and guidance from the IC/UC.

As shown in Figure 6, the Planning Section is comprised of four primary Units, as well as a number of technical specialists to assist in evaluating the situation, developing planning options, and forecasting requirements for additional resources. Within the Planning Section, the following primary Units fulfill functional requirements:

- ***Resources Unit:*** Responsible for recording the status of resources committed to the incident. This Unit also evaluates resources committed currently to the incident, the effects additional responding resources will have on the incident, and anticipated resource needs.
- ***Situation Unit:*** Responsible for the collection, organization, and analysis of incident status information, and for analysis ao the situation as it progresses.
- ***Demobilization Unit:*** Responsible for ensuring orderly, safe, and efficient demobilization of incident resources.
- ***Documentation Unit:*** Responsible for collecting, recording, and safeguarding all documents relevant to the incident.
- ***Technical Specialist(s):*** Personnel with special skills that can be used anywhere within the ICS organization.

Figure 6. Planning Section Organization



The Planning Section is normally responsible for gathering and disseminating information and intelligence critical to the incident, unless the IC/UC places this function elsewhere. The

Planning Section is also responsible for assembling the IAP. The IAP includes the overall incident objectives and strategies established by Incident Command. In the case of a UC, the IAP must adequately address the mission and policy needs of each jurisdictional agency, as well as interaction between jurisdictions, functional agencies, and private organizations. The IAP also addresses tactics and support activities required for the planned operational period, generally 12 to 24 hours.

The IAP should incorporate changes in strategies and tactics based on lessons learned during earlier operational periods. A written IAP is especially important when:

- Resources from multiple agencies and/or jurisdictions are involved;
- The incident will span several operational periods;
- Changes in shifts of personnel and/or equipment are required; or
- There is a need to document actions and decisions.

The IAP will typically contain a number of components, as shown in Table 5. **Table 5. Sample IAP Outline**

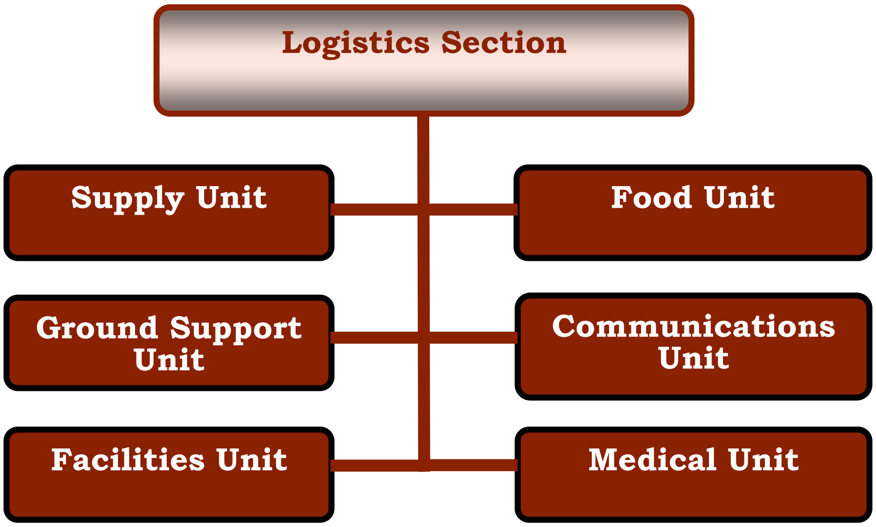
Component	**Normally Prepared By:**
Incident Objectives	Incident Commander
Organization Assignment List or Chart	Resource Unit
Assignment List	Resource Unit
Incident Radio Communications Plan	Communication Unit
Medical Plan	Medical Unit
Incident Maps	Situation Unit
General Safety Message/Site Safety Plan	Safety Officer
Other Potential Components (incident dependent)	
Air Operations Summary	Air Operations
Traffic Plan	Ground Support Unit
Decontamination Plan	Technical Specialist
Waste Management or Disposal Plan	Technical Specialist
Demobilization Plan	Demobilization Unit
Site Security Plan	Law Enforcement, Technical Specialist, or Security Manager
Investigative Plan	Low Enforcement
Evidence Recovery Plan	Low Enforcement
Evakuation Plan	As Required
Sheltering/Mass Care Plan	As Required
Other (as required)	As Required

c. Logistics Section

The Logistics Section (see Figure 7) is responsible for all service support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. This Section also provides facilities, security (of the incident command facilities and personnel), transportation, supplies, equipment maintenance and fuel, food services, communications and information technology support, and emergency responder medical services, including inoculations, as required. Within the Logistics Section, six primary Units fulfill functional requirements:

- *Supply Unit:* Orders, receives, stores, and processes all incident-related resources, personnel, and supplies.
- *Ground Support Unit:* Provides all ground transportation during an incident. In conjunction with providing transportation, the Unit is also responsible for maintaining and supplying vehicles, keeping usage records, and developing incident Traffic Plans.
- *Facilities Unit:* Sets up, maintains, and demobilizes all facilities used in support of incident operations. The Unit also provides facility maintenance and security services required to support incident operations.
- *Food Unit:* Determines food and water requirements, plans menus, orders food, provides cooking facilities, cooks, serves, maintains food service areas, and manages food security and safety concerns.
- *Communications Unit:* Major responsibilities include effective communications planning as well as acquiring, setting up, maintaining, and accounting for communications equipment.
- *Medical Unit:* Responsible for the effective and efficient provision of medical services to incident personnel.

Figure 7. Logistics Section Organization



d. Finance/Administration Section

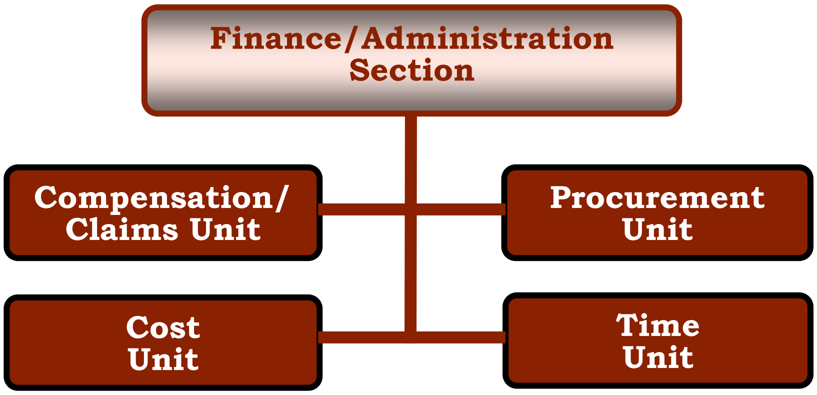
A Finance/Administration Section is established when the incident management activities require on-scene or incident-specific finance and other administrative support services. Some of the functions that fall within the scope of this Section are recording personnel time, maintaining vendor contracts, administering compensation and claims, and conducting an overall cost analysis for the incident. If a separate Section is established, close coordination with the

Planning Section and Logistics Section is also essential so that operational records can be reconciled with financial documents.

The Finance/Administration Section is a critical part of ICS in large, complex incidents involving significant funding originating from multiple sources. In addition to monitoring multiple sources of funds, the Section Chief must track and report to Incident Command the accrued cost as the incident progresses. This allows the IC/UC to forecast the need for additional funds before operations are negatively affected. Figure 8 illustrates the basic organizational structure for a Finance/Administration Section. When such a Section is established, the depicted Units may be staffed as required. Within the Finance/Administration Section, four primary Units fulfill functional requirements:

- ***Compensation/Claims Unit:*** Responsible for financial concerns resulting from property damage, injuries, or fatalities at the incident.
- ***Cost Unit:*** Responsible for tracking costs, analyzing cost data, making estimates, and recommending cost savings measures.
- ***Procurement Unit:*** Responsible for financial matters concerning vendor contracts.
- ***Time Unit:*** Responsible for recording time for incident personnel and hired equipment.

Figure 8. Finance/Administration Section Organization



e. Intelligence/Investigations Function

The collection, analysis, and sharing of incident-related intelligence are important elements of ICS. Normally, operational information and situational intelligence are management functions located in the Planning Section, with a focus on three incident intelligence areas: situation status, resource status, and anticipated incident status or escalation (e.g., weather forecasts and location of supplies). This information and intelligence is utilized for incident management decision-making. In addition, technical specialists in the Planning Section may be utilized to provide specific information that supports tactical decisions.

Incident management organizations must also establish a system for the collection, analysis, and sharing of information developed during intelligence/investigation efforts. Some incidents require intelligence and investigative information, which is defined in either of two ways. First, it is defined as information that leads to the detection, prevention, apprehension, and prosecution of criminal activities or the individuals involved, including terrorist incidents. Second, it is defined as information that leads to determination of the cause, projection of spread, assessment of impact, or selection of countermeasures for a given incident (regardless of the source) such as public health events, disease outbreaks, or fires with unknown origins.

ICS allows for organizational flexibility, so the Intelligence/Investigations Function can be embedded in several different places within the organizational structure.

- ***Within the Planning Section:*** This is the traditional placement for this function and is appropriate for incidents with little or no investigative information requirements nor a significant amount of specialized information.
- ***As a Separate General Staff Section:*** This option may be appropriate when a there is a significant intelligence/investigations component to the incident for criminal or epidemiological purposes or when multiple investigative agencies are involved. A separate Intelligence/Investigations Section may be needed when highly specialized
- Information requiring technical analysis is both critical and time sensitive to lifesaving operations (e.g., chemical, biological, radiological, or nuclear incidents) or when there is a need for classified intelligence.
- ***Within the Operations Section:*** This option may be appropriate for incidents that require a high degree of linkage and coordination between the investigative information and the operational tactics that are being employed.
- ***Within the Command Staff:*** This option may be appropriate for incidents with little need for tactical information or classified intelligence and where supporting Agency Representatives are providing real-time information to the IC/UC.

The mission of the Intelligence/Investigations Function is to ensure that all investigative and intelligence operations, functions, and activities within the incident response are properly managed, coordinated, and directed in order to:

- Prevent/deter additional activity, incidents, or attacks.
- Collect, process, analyze, and appropriately disseminate intelligence information.
- Conduct a thorough and comprehensive investigation.
- Identify, process, collect, create a chain of custody for, safeguard, examine/analyze, and store all probative evidence.
- Determine source or cause and control spread and impact, in the investigation of emerging incidents (fire, disease outbreak, etc.).

The Intelligence/Investigations Function has responsibilities that cross all interests of departments involved during an incident; however, certain functions remain specific to law enforcement response and mission areas. Two examples of these are to expeditiously identify and apprehend all perpetrators, and to successfully prosecute all defendants.

Regardless of how the Intelligence/Investigations Function is organized, a close liaison will be maintained, and information will be transmitted to Incident Command, the Operations Section, and the Planning Section. However, classified information requiring a security clearance, sensitive information, or specific investigative tactics that would compromise the investigation will be shared only with those who have the appropriate security clearance or a need to know.

The Intelligence/Investigations Function can be organized in a variety of ways. The following are examples of Groups that may be activated if needed:

- ***Investigative Operations Group:*** Responsible for overall investigative effort.
- ***Intelligence Group:*** Responsible for obtaining unclassified, classified, and open source intelligence.
- ***Forensic Group:*** Responsible for collection and integrity of forensic evidence, and in incidents of a criminal nature, the integrity of the crime scene.
- ***Investigative Support Group:*** Responsible for ensuring that required investigative personnel are made available expeditiously and that the necessary resources are properly distributed, maintained, safeguarded, stored, and returned, when appropriate.

Other Groups may be created to handle the following responsibilities: ensuring that missing or unidentified persons and human remains are investigated and identified expeditiously and that required notifications are made in a timely manner. These responsibilities include the collection of ante mortem information and exemplars in a family assistance center.

4. INCIDENT MANAGEMENT TEAMS

An IMT is an incident command organization made up of the Command and General Staff members and other appropriate personnel in an ICS organization and can be deployed or activated, as needed. Central, regional, and some local IMTs have formal certification and qualification, notification, deployment, and operational procedures in place. In other cases, IMTs are formed at an incident or for specific events. The level of training and experience of the IMT members, coupled with the IMT's identified formal response requirements and responsibilities, are factors in determining an IMT's type, or level.

6. REGIONAL COMMAND

a. Description

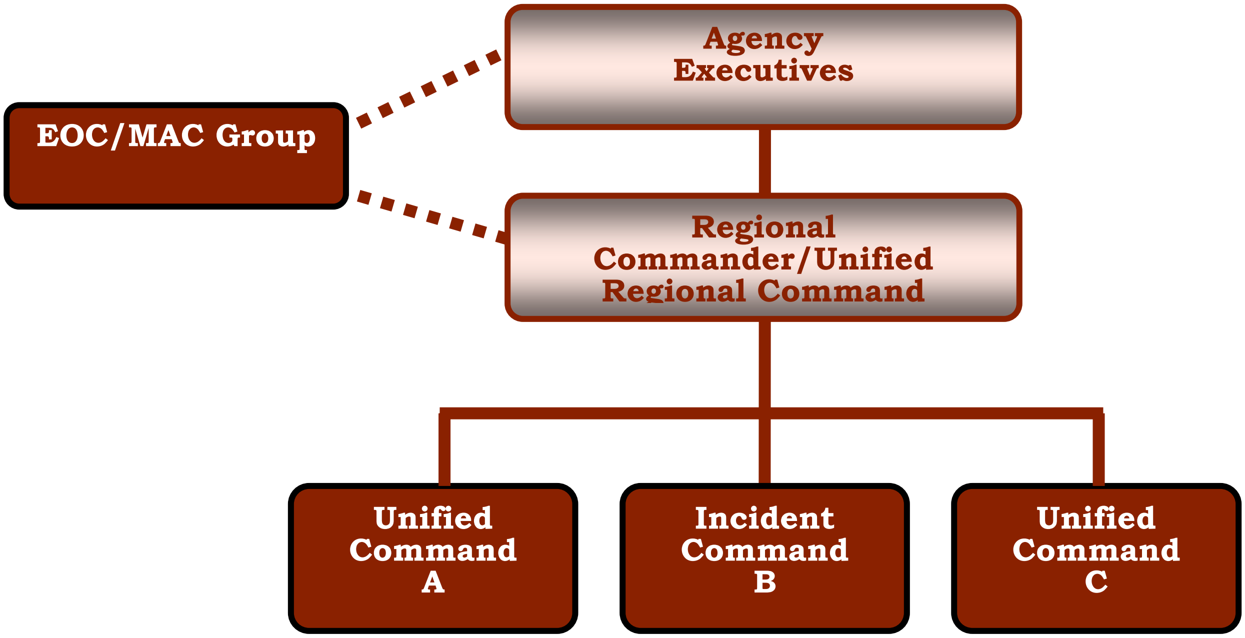
Area Command is an organization to oversee the management of multiple incidents handled individually by separate ICS organizations or to oversee the management of a very large or evolving incident engaging multiple IMTs. An Agency Executive or other public official with jurisdictional responsibility for the incident usually makes the decision to establish a Regional Command. A Regional Command is activated only if necessary, depending on the complexity of the incident and incident management span-of-control considerations.

Regional Commands are particularly relevant to incidents that are typically not site specific, are not immediately identifiable, are geographically dispersed, and evolve over longer periods of time (e.g., public health emergencies, earthquakes, tornadoes, civil disturbances, and any geographic area where several IMTs are being used and these incidents are all requesting similar resources). Incidents such as these, as well as acts of biological, chemical, radiological, and nuclear terrorism, require a coordinated intergovernmental, NGO, and private-sector response, with large-scale coordination typically conducted at a higher jurisdictional level. Regional Command is also used when a number of incidents of the same type in the same area are competing for the same resources, such as multiple hazardous material incidents, spills, or fires.

When incidents are of different types and/or do not have similar resource demands, they are usually handled as separate incidents or are coordinated through an Emergency Operations Center (EOC) or Multiagency Coordination Group (MAC Group). If the incidents under the authority of the Regional Command span multiple jurisdictions, a Unified Regional Command should be established (see Figure 9). This allows each jurisdiction to have appropriate representation in the Regional Command.

Regional Command should not be confused with the functions performed by MACS: Regional Command oversees management coordination of the incident(s), while a MACS element, such as a communications/dispatch center, EOC, or MAC Group, coordinates support.

Figure 9. Chain of Command and Reporting Relationships



b. Responsibilities

For incidents under its authority, a Regional Command has the following responsibilities:

- Develop broad objectives for the impacted area(s).
- Coordinate the development of individual incident objectives and strategies.

- (Re) allocate resources as the established priorities change.
- Ensure that incidents are properly managed.
- Ensure effective communications.
- Ensure that incident management objectives are met and do not conflict with each other or with agency policies.
- Identify critical resource needs and report them to the established EOC/MAC Groups.
- Ensure that short-term "emergency" recovery is coordinated to assist in the transition to full recovery operations.

B. MULTIAGENCY COORDINATION SYSTEMS

Multiagency coordination is a **process** that allows all levels of government and all disciplines to work together more efficiently and effectively. Multiagency coordination occurs across the different disciplines involved in incident management, across jurisdictional lines, or across levels of government.

Multiagency coordination can and does occur on a regular basis whenever personnel from different agencies interact in such activities as preparedness, prevention, response, recovery, and mitigation. Often, cooperating agencies develop a MACS to better define how they will work together and to work together more efficiently; however, multiagency coordination can take place without established protocols. MACS may be put in motion regardless of the location, personnel titles, or organizational structure. MACS includes planning and coordinating resources and other support for planned, notice, or no-notice events. MACS defines business practices, standard operating procedures, processes, and protocols by which participating agencies will coordinate their interactions. Integral elements of MACS are dispatch procedures and protocols, the incident command structure, and the coordination and support activities taking place within an activated EOC. Fundamentally, MACS provide support, coordination, and assistance with policy-level decisions to the ICS structure managing an incident.

Written agreements allow agencies within the system to conduct activities using established rules and are often self-defined by the participating organizations. A fully implemented MACS is critical for seamless multiagency coordination activities and essential to the success and safety of the response whenever more than one jurisdictional agency responds. Moreover, the use of MACS is one of the fundamental components of Command and Management within IEMS, as it promotes scalability and flexibility necessary for a coordinated response.

1. DEFINITION

The primary function of MACS is to coordinate activities above the field level and to prioritize the incident demands for critical or competing resources, thereby assisting the coordination of the operations in the field. MACS consist of a combination of elements: personnel, procedures, protocols, business practices, and communications integrated into a common system. For the purpose of coordinating resources and support between multiple jurisdictions, MACS can be implemented from a fixed facility or by other arrangements outlined within the system.

In some instances, MACS is informal and based on oral agreements between jurisdictions, but usually it is more formalized and supported by written agreements, operational procedures, and protocols. The formal process, where issues are addressed before an incident occurs, is the preferred and recommended approach, as it streamlines the coordination function. While ad hoc arrangements between jurisdictions may result in effective multiagency coordination on relatively minor incidents, coordination on larger, more complex incidents is most successful when it takes place within a planned and well-established system.

2. SYSTEM ELEMENTS

MACS includes a combination of facilities, equipment, personnel, and procedures integrated into a common system with responsibility for coordination of resources and support to emergency operations.

a. Facilities

The need for location(s) (such as a communications/dispatch center, EOC, city hall, virtual location) to house system activities will depend on the anticipated functions of the system.

b. Equipment

To accomplish system activities, equipment (such as computers and phones) must be identified and procured.

c. Personnel

Typical personnel include Agency Executives, or their appointed representatives, who are authorized to commit agency resources and funds in a coordinated response effort. Personnel can also be authorized representatives from supporting agencies, NGOs, and the private sector who assist in coordinating activities above the field level.

d. Procedures

Procedures include processes, protocols, agreements, and business practices that prescribe the activities, relationships, and functionality of the MACS. Identifying the interactive communications activities and associated implementation plans are critical components of the system.

3. EXAMPLES OF SYSTEM ELEMENTS

The two most commonly used elements of the Multiagency Coordination System are EOCs and MAC Groups.

a. Emergency Operations Center

EOCs may be organized by major discipline (e.g., fire, law enforcement, or emergency medical services); by emergency support function (e.g., transportation, communications, public works and engineering, or resource support); by jurisdiction (e.g., city, county, or region); or, more likely, by some combination thereof. ICPs need good communication links to EOCs to ensure effective and efficient incident management.

Often, agencies within a political jurisdiction will establish coordination, communications, control, logistics, etc., at the department level for conducting overall management of their assigned resources. Governmental departments (or agencies, bureaus, etc.) or private organizations may also have operations centers (referred to here as Department Operations Centers, or DOCs) that serve as the interface between the ongoing operations of that organization and the emergency operations it is supporting. The DOC may directly support the incident and receive information relative to its operations. In most cases, DOCs are physically represented in a combined agency EOC by authorized agent(s) for the department or agency.

EOCs may be staffed by personnel representing multiple jurisdictions and functional disciplines and a wide variety of resources. For example, a local EOC established in response to a bioterrorism incident would likely include a mix of law enforcement, emergency management, public health, and medical personnel (local, State, or Central public health officials and possibly representatives of health care facilities, emergency medical services, etc.).

The physical size, staffing, and equipping of an EOC will depend on the size of the jurisdiction, resources available and anticipated incident management workload. EOCs may be organized and staffed in a variety of ways. Regardless of its specific organizational structure, an EOC should include the following core functions: coordination; communications; resource allocation and tracking; and information collection, analysis, and dissemination.

Upon activation of a local EOC, communications and coordination must be established between Incident Command and the EOC. ICS field organizations must also establish communications with the activated local EOC, either directly or through their parent organizations. Additionally,

EOCs at all levels of government and across functional agencies must be capable of communicating appropriately with other EOCs, including those maintained by private organizations. Communications between EOCs must be reliable and contain built-in redundancies. The efficient functioning of EOCs most frequently depends on the existence of mutual aid agreements and joint communications protocols among participating agencies.

b. MAC Group

Typically, Agency Executives, or their designees, who are authorized to represent or commit agency resources and funds are brought together to form MAC Groups. MAC Groups may also be known as multiagency committees, emergency management committees, or as otherwise defined by the system. Personnel assigned to the EOC who meet the criteria for participation in a MAC Group may be asked to fulfill that role.

A MAC Group does not have any direct incident involvement and will often be located some distance from the incident site(s). In many cases a MAC Group can function virtually to accomplish its assigned tasks.

A MAC Group may require a support organization for its own logistics and documentation needs; to manage incident-related decision support information such as tracking critical resources, situation status, and intelligence or investigative information; and to provide public information to the news media and public. The number and skills of its personnel will vary by incident complexity, activity levels, needs of the MAC Group, and other factors identified through agreements or by preparedness organizations. A MAC Group may be established at any level (e.g., national, State, or local) or within any discipline (e.g., emergency management, public health, critical infrastructure, or private sector).

4. PRIMARY FUNCTIONS OF MACS

The Multiagency Coordination System should be both flexible and scalable to be efficient and effective. MACS will generally perform common functions during an incident; however, not all of the system's functions will be performed during every incident, and functions may not occur in any particular order.

a. Situation Assessment

This assessment includes the collection, processing, and display of all information needed. This may take the form of consolidating situation reports, obtaining supplemental information, and preparing maps and status boards.

b. Incident Priority Determination

Establishing the priorities among ongoing incidents within the defined area of responsibility is another component of MACS. Typically, a process or procedure is established to coordinate with Area or Incident Commands to prioritize the incident demands for critical resources. Additional considerations for determining priorities include the following:

- Life-threatening situations.
- Threat to property.
- High damage potential.
- Incident complexity.
- Environmental impact.
- Economic impact.

- Other criteria established by the Multiagency Coordination System.

c. Critical Resource Acquisition and Allocation

Designated critical resources will be acquired, if possible, from the involved agencies or jurisdictions. These agencies or jurisdictions may shift resources internally to match the incident needs as a result of incident priority decisions. Resources available from incidents in the process of demobilization may be shifted, for example, to higher priority incidents.

Resources may also be acquired from outside the affected area. Procedures for acquiring outside resources will vary, depending on such things as the agencies involved and written agreements.

d. Support for Relevant Incident Management Policies and Interagency Activities

A primary function of MACS is to coordinate, support, and assist with policy-level decisions and interagency activities relevant to incident management activities, policies, priorities, and strategies.

e. Coordination with other MACS Elements

A critical part of MACS is outlining how each system element will communicate and coordinate with other system elements at the same level, the level above, and the level below. Those involved in multiagency coordination functions following an incident may be responsible for incorporating lessons learned into their procedures, protocols, business practices, and communications strategies. These improvements may need to be coordinated with other appropriate preparedness organizations.

f. Coordination With Elected and Appointed Officials

Another primary function outlined in MACS is a process or procedure to keep elected and appointed officials at all levels of government informed. Maintaining the awareness and support of these officials, particularly those from jurisdictions within the affected area, is extremely important, as scarce resources may need to move to an agency or jurisdiction with higher priorities.

g. Coordination of Summary Information

By virtue of the situation assessment function, personnel implementing the multiagency coordination procedures may provide summary information on incidents within their area of responsibility as well as provide agency/jurisdictional contacts for media and other interested agencies.

C. PUBLIC INFORMATION

1. INTRODUCTION

Public Information consists of the processes, procedures, and systems to communicate timely, accurate, and accessible information on the incident's cause, size, and current situation to the public, responders, and additional stakeholders (both directly affected and indirectly affected). Public information must be coordinated and integrated across jurisdictions, agencies, and organizations; among Central, State, tribal, and local governments; and with NGOs and the private sector. Well-developed public information, education strategies, and communications plans help to ensure that lifesaving measures, evacuation routes, threat and alert systems, and other public safety information are coordinated and communicated to numerous audiences in a timely, consistent manner.

2. SYSTEM DESCRIPTION AND COMPONENTS

a. Public Information Officer

The Public Information Officer supports the incident command structure as a member of the Command staff. The Public Information Officer advises the IC/UC on all public information matters relating to the management of the incident. The Public Information Officer also handles inquiries from the media, the public, and elected officials; emergency public information and warnings; rumor monitoring and response; media relations; and other functions required to gather, verify, coordinate, and disseminate accurate, accessible, and timely information related to the incident. Information on public health, safety, and protection is of particular importance.

Public Information Officers are able to create coordinated and consistent messages by collaborating to:

- Identify key information that needs to be communicated to the public.
- Craft messages conveying key information that are clear and easily understood by all, including those with special needs.

- Prioritize messages to ensure timely delivery of information without overwhelming the audience.
- Verify accuracy of information through appropriate channels.
- Disseminate messages using the most effective means available.

b. Joint Information System

The Joint Information System (JIS) provides the mechanism to organize, integrate, and coordinate information to ensure timely, accurate, accessible, and consistent messaging across multiple jurisdictions and/or disciplines with NGOs and the private sector. The JIS includes the plans, protocols, procedures, and structures used to provide public information. Public Information Officers of all levels and established JICs are critical supporting elements of the JIS. Key elements include the following:

- Interagency coordination and integration.
- Gathering, verifying, coordinating, and disseminating consistent messages.
- Support for decision makers.
- Flexibility, modularity, and adaptability.

c. Joint Information Center

The JIC is a central location that facilitates operation of the JIS, where personnel with public information responsibilities perform critical emergency information functions, crisis communications, and public affairs functions. JICs may be established at various levels of government or at incident sites, or can be components of Central, State, tribal, territorial, regional, or local MACS (e.g., MAC Groups or EOCs). Depending on the requirements of the incident, an incident-specific JIC is typically established at a single, on-scene location in coordination with central, regional and local agencies or at the national level if the situation warrants. Releases are cleared through the IC/UC, EOC/MAC Group, and/or Central officials in the case of centrally coordinated incidents to ensure consistent messages, avoid release of conflicting information, and prevent negative impact on operations. This formal process for releasing information ensures the protection of incident-sensitive information. Agencies may issue their own releases related to their policies, procedures, programs, and capabilities; however, these should be coordinated with the incident-specific JIC(s).

A single JIC location is preferable, but the system is flexible and adaptable enough to accommodate multiple physical or virtual JIC locations. For example, multiple JICs may be needed for a complex incident spanning a wide geographic area or multiple jurisdictions. In instances when multiple JICs are activated, information must be coordinated among all appropriate JICs; each JIC must have procedures and protocols to communicate and coordinate effectively with one another. Whenever there are multiple JICs, the final release authority must be the senior command, whether using Unified or Area Command structures. A national JIC may be used when an incident requires central coordination and is expected to be of long duration (e.g., weeks or months) or when the incident affects a large area of the country.

JICs can be organized in many ways, depending on the nature of the incident. Table 7 identifies several types of JICs.

Table 7. Types of Joint Information Centers

Incident	• Optimal physical location for local and IC-assigned Public Information Officers to co-locate • Easy media access is paramount to success
Virtual	• Established when physical co-location is not feasible • Incorporates technology and communication protocols
Satellite	• Smaller in scale than other JICs • Established primarily to support the incident JIC • Operates under the control of the primary JIC for that incident • Is not independent of that direction
Area	• Supports wide-area multiple-incident ICS structures • Could be established on a local or statewide basis • Media access is paramount
Support	• Established to support several incident JICs in multiple States • Offers supplemental staff and resources outside of the disaster area
National	• Established for long-duration incidents • Established to support Central response activities • Staffed by numerous Central departments and/or agencies

d. Organizational Independence

Organizations participating in incident management retain their independence. Incident Command and MACS are responsible for establishing and overseeing JICs, including processes for coordinating and clearing public communications. In the case of Unified Command, the departments, agencies, organizations, or jurisdictions that contribute to joint public information management do not lose their individual identities or responsibility for their own programs or policies. Rather, each agency/organization contributes to the overall unified message.

e. Getting Information to the Public and Additional Stakeholders

The process of getting information to the public and additional stakeholders during an incident is an ongoing cycle that involves four steps.

(1) Gathering Information

Gathering information is the first step in the process of getting information to the public and additional stakeholders. Information is collected from:

- ***On-Scene Command:*** A source of ongoing, official information on the response effort.
- ***On-Scene Public Information Officers:*** Report to the JIC what they are observing and hearing at the incident from the news media, elected officials and their staff, and the public.
- ***Media Monitoring:*** Used to assess the accuracy and content of news media reports. It also helps to identify trends and breaking issues.
- ***News Media:*** A valuable source of developing information and current issues.

- ***Public and Elected/Appointed Officials:*** Inquiries from elected/appointed officials, community leaders, and the general public point to the specific concerns of those in the affected areas.

(2) Verifying Information

The next step in the process is to verify the accuracy of the information that has been collected, by consulting the following sources:

- ***Other Public Information Officers in the JIC:*** Comparing notes—especially with the lead Public Information Officer and Public Information Officers who are liaisons to the various assistance programs or response/recovery partners—is one way to verify information accuracy.
- ***EOC Sources:*** Including program leads, who should be asked to confirm information.
- ***On-Scene Public Information Officers:*** A valuable source for checking the accuracy of information reported to the EOC with reports from the news media, the offices of elected officials, and people on the scene.

(3) Coordinating Information

The next step in the process is to coordinate with other Public Information Officers who are part of the JIS. These Public Information Officers include both those represented in the JIC and those working from another location who are part of the JIS. Coordinating information involves:

- ***Establishing Key Message(s):*** After gathering information from all sources, unified messages are crafted that address all informational needs and are prioritized according to the overall Central, State, tribal, and local response/recovery strategy. The mission includes getting accurate, consistent information to the right people at the right time so they can make informed decisions.
- ***Obtaining Approval/Clearance From Those With Authority:*** Ensuring that the information is consistent, accurate, and accessible. The approval process should be streamlined, however, to ensure that the information is released in a timely manner.

(4) Disseminating Information

The next step in the process is to disseminate information to the public and additional stakeholders. This step involves:

- ***Using Multiple Methods:*** In an emergency, there may not be many options. Phone calls and interviews might be the primary means of getting information to the news media. Personal visits or town meetings may be the most effective avenue for the public, elected/appointed officials, or other stakeholders. These outreach efforts can be supported by providing talking points and fliers to on-scene Public Information Officers.
- ***Monitoring the Media:*** Media monitoring is invaluable for ensuring that the message is understood by the news media and reported accurately and completely. Important inaccuracies should be addressed before they are reported incorrectly a second time.

3. PUBLIC INFORMATION COMMUNICATIONS PLANNING

Information communications strategies and planning are essential to all aspects of public information. Plans should include processes, protocols, and procedures that require the development of draft news releases; media lists; and contact information for elected/appointed officials, community leaders, private-sector organizations, and public service organizations to facilitate the dissemination of accurate, consistent, accessible, and timely public information. Public information communications should be a critical component of training and exercises.

D. RELATIONSHIPS AMONG COMMAND AND MANAGEMENT ELEMENTS

ICS, MACS, and Public Information have been described herein as separate elements of Command and Management within IEMS. However, IEMS relies on the relationships among these elements along with the elements themselves.

Some relationships are specifically defined. For example, a Regional Command or Incident Command coordinates with Public Information on incident-specific public information through an incident Public Information Officer within the JIS. The relationship between Regional Command or Incident Command and MACS is primarily defined by a communications link between Command and/or field-level personnel with resource management responsibilities and a particular staff position within multiagency coordination.

These relationships—along with other relationships among Command and Management elements that are not as clearly defined in advance—must be clearly defined and documented as each element evolves during an incident.

COMPONENT V:

ONGOING MANAGEMENT AND MAINTENANCE

The Ongoing Management and Maintenance component of IEMS contains two subsections: the Emergency Management Institute (EMI) and Supporting Technologies. The EMI section of the document sets forth the responsibilities of the EMI. The Supporting Technologies Section discusses principles necessary to leverage science and technology to improve capabilities and lower costs.

A. EMERGENCY MANAGEMENT INSTITUT

The EMI provides strategic direction for and oversight of IEMS, supporting routine maintenance and continuous refinement of the system and its components over the long term. The EMI solicits participation from ministries and central agencies; regional authorities, and local governments; and emergency management/response personnel, including those from NGOs and the private sector. Revisions to IEMS and other issues can be proposed by all IEMS users (including governments at all levels, as well as the private sector, voluntary organizations, academia, nonprofit organizations, and other IEMS-related professional associations). Additionally, the EMI administers IEMS compliance requirements, facilitates the development of guidance standards for typing and credentialing, supports IEMS training and exercises, and manages the publication of various IEMS-related materials.

1. CONCEPTS AND PRINCIPLES

The process for managing and maintaining IEMS ensures that all users and stakeholders—including all levels of government, functional disciplines, NGOs, and the private sector—are given the opportunity to participate in EMI activities. The IEMS management and maintenance process relies heavily on lessons learned from actual incidents and incident management training and exercises, as well as recognized best practices across jur and functional disciplines.

2. IEMS REVISION PROCESS

The IEMS document will be reviewed on a 2-year cycle and revised to incorporate new directives, legislative changes, and procedural changes based on lessons learned from exercises, actual incidents, and planned events. Proposed changes to IEMS will be submitted to the EMI for consideration, approval, and publication.

The Minister is responsible for publishing revisions and modifications to IEMS-related documents, including supplementary standards, procedures, and other materials, and will do so with regular consultation with other ministries, departments and agencies and local governments.

3. EMI RESPONSIBILITIES

a. Administration and Compliance

To manage ongoing administration and implementation of IEMS, including specification of compliance measures, the EMI is responsible for working toward the following:

- Developing and maintaining a national program for IEMS education and awareness, including specific instruction on the purpose and content of this document and IEMS in general.
- Promoting compatibility between national-level standards for IEMS and those developed by other public, private, and professional groups.
- Facilitating the establishment and maintenance of a documentation and database system related to qualification, certification, and credentialing of emergency management/response personnel and organizations that includes reviewing and approving discipline-specific requirements
- Developing assessment criteria for the various components of IEMS.

b. Standards and Credentialing

The EMI will work with appropriate standards development organizations to ensure the adoption of common national standards and credentialing systems that are compatible and aligned with the implementation of IEMS. Identification, adoption, and development of common standards and credentialing programs include the following:

- Facilitating the development and publication of national standards, guidelines, and protocols for the qualification, licensure, and certification of emergency management/response personnel, as appropriate.
- Reviewing and approving discipline-specific qualification and certification requirements.

- Establishing a data maintenance system to provide incident managers with the detailed qualification, experience, and training information needed to credential personnel for prescribed national incident management positions.
- Coordinating minimum professional certification standards and facilitating the design and implementation of a nationwide credentialing system.
- Facilitating the establishment of standards for the performance, compatibility, and interoperability of incident management equipment and communications systems, including the following:
    - Facilitating the development and publication of national standards, guidelines, and protocols for equipment certification, including the incorporation of existing standards and certification programs used by incident management and emergency response organizations nationwide.
    - Reviewing and approving lists of equipment that meet these established equipment certification requirements.
    - Collaborating with organizations responsible for emergency-responder equipment evaluation and testing.

- Facilitating the development and issuance of national standards for resource typing.
- Facilitating the definition and maintenance of the information framework required for the development of IEMS information systems, including the development of data standards.
- Coordinating the establishment of technical and technology standards for IEMS users.

c. Training and Exercise Support

To lead the development of training and exercises that further appropriate agencies' and organizations' knowledge, adoption, and implementation of IEMS, the EMI will coordinate with them to do the following:

- Facilitate the definition of general training requirements and the development of national-level training standards and course curricula associated with IEMS, including the following:

    - The use of modeling and simulation capabilities for training and exercise programs.
    - Field-based training, specification of mission-essential tasks, requirements for specialized instruction and instructor training, and course completion documentation for all IEMS users.
    - The review and recommendation (in coordination with Central, State, tribal, local, nongovernmental, private-sector, and national professional organizations) of discipline-specific IEMS training courses.

- Facilitate the development of national standards, guidelines, and protocols for incident management training and exercises, including consideration of existing exercise and training programs at all jurisdictional levels.

- Facilitate the development of training necessary to support the incorporation of IEMS across all jurisdictional levels.
- Establish and maintain a repository for reports and lessons learned from actual incidents, training, and exercises, as well as for best practices, model structures, and processes for IEMS-related functions.

d. Publication Management

Publication management for IEMS includes the development of naming and numbering conventions, the review and certification of publications, development of methods for publications control, identification of sources and suppliers for publications and related services, management of publication distribution, and assurance of product accessibility.

IEMS publication management includes the following types of products:

- Qualifications information.
- Training course and exercise information.
- Task books.
- Incident Command System training, forms, and templates (and other necessary forms).
- Job aids and guides.
- Computer programs.
- Audio and video resources.
- Best-practices manuals/models/recommendations.

To manage IEMS-related publications, the EMI will coordinate with appropriate agencies and organizations and take the lead on the following:

- Facilitating the establishment and maintenance of a publication management system for IEMS-related publications and materials, including the development or coordination of general publications for all IEMS users.
- Issuing documents or information by means of the IEMS publication management system.
- Facilitating the development and publication of standardized templates and materials, such as supplementary documentation and desk guides, to support the implementation and continuous refinement of IEMS.
- Reviewing discipline-specific publication management requirements.

B. SUPPORTING TECHNOLOGIES

Ongoing development of science and technology is integral to the continual improvement and refinement of IEMS. Strategic R&D ensures that this development takes place. IEMS also relies on scientifically based technical standards that support incident management. Maintaining a focus on appropriate science and technology solutions will necessitate a long-term collaborative effort among IEMS partners.

To ensure the effective development of incident-management science and technology solutions, the NIC must work in coordination with the Science and Technology Sector to assess the needs of emergency management/response personnel and their affiliated organizations.

1. CONCEPTS AND PRINCIPLES

IEMS leverages science and technology to improve capabilities and lower costs. It observes the five key principles defined below.

a. Interoperability and Compatibility

Systems operating in an incident management environment must be able to interact smoothly across disciplines and jurisdictions. Interoperability and compatibility are achieved through the use of tools such as common communications and data standards, digital data formats, equipment standards, and design standards.

b. Technology Support

Technology support is the use and incorporation of new and existing technologies to improve efficiency and effectiveness in all aspects of incident management. Technology support permits organizations using IEMS to enhance all aspects of emergency management and incident response.

c. Technology Standards

Supporting systems and technologies are based on requirements developed in collaboration with Central, State, tribal, and local governments, as well as NGOs, the private sector, and national professional organizations. National standards may be required to facilitate the interoperability and compatibility of key systems across jurisdictions and/or disciplines.

d. Broad-Based Requirements

Needs for new technologies, procedures, protocols, and standards to facilitate incident management are identified before, during, and after an incident. As these needs could exceed available resources, IEMS provides a mechanism for aggregating and prioritizing needs and resources. These needs will be met by coordinating testing and evaluation activities for basic, applied, developmental, and demonstration-based research.

ANNEX. I

Legal framework and International Instruments

1. Constitution of the Republic of Kosova
2. Law on Natural and other disasters Nr.2006/02/L-68;
3. Law on Kosovo Security Council Nr.2008/03-L050;
4. Law on Fire Protection Nr.2006/02-L41;
5. Law on Public Finance Management and responsibilities Nr.2008/03-L048;
6. Law on Ministry of Kosovo Security Force Nr.2008/03-L045;
7. Law on Police Nr. 03/L-035;
8. Law on Telecommunication Nr.2002/7;
9. Law on Traffic Transportation Nr. 2004/1;
10. Law on Public Health Nr. 02/L-78;
11. Law on Emergency Health Care Nr.2006/02-L50;
12. Law on Kosovo Red Cross Nr.03/L-179
13. Law on Supplementing and Amending of the Criminal Code of Kosovo Nr.2008/03-L-002;
14. Law on Supplementing and Amending of the Kosovo Code of Criminal Procedure Nr.2008/03-L-002;
15. Law on Contentious Procedure Nr.03/L-006;
16. Law on Non-Contentious Procedure Nr.03/L-007;
17. Law on Public Enterprises Nr.2008/03-L087;
18. Law on Local Governance Nr.2008/03-L040;
19. Administrative Instruction on Criteria for Establishment and organisation of the Fire-Fighting and Rescue Service in Kosovo Nr.05/2007;
20. Administrative Instruction on the Methodology of composition of risk assessment and plans for protection and rescue Nr.19/2008;
21. Administrative Instruction on creation of the Traffic Safety council Nr.18/2008;
22. Working Regulation of the Kosovo Security Council
23. Working Regulation of the Situation Centre

Republika e Kosovës
Republika Kosova-Republic of Kosovo
Qeveria - Vlada - Government

Nr. 12/126
Datë: 26.05.2010

Në mbështetje të nenit 92 paragrafi 4. dhe 93 paragrafi (4) të Kushtetutës së Republikës së Kosovës, dhe paragrafit (3) të nenit 4 të Rregullores së Punës së Qeverisë së Kosovës nr. 01/2007, Qeveria e Republikës së Kosovës, në mbledhjen e mbajtur më 26 maj 2010, mori

VENDIM

1. Miratohet Sistemi i Integruar i Menaxhimit të Emergjencave.

2. Për zbatimin e këtij Vendimi ngarkohet Ministria e Punëve të Brendshme.

3. Vendimi hyn në fuqi ditën e nënshkrimit.

Hashim THAÇI

Kryeministër i Kosovës

Iu dërgohet:
- të gjitha ministrive (ministrave)
- Sekretarit të Përhershëm të ZKM-ës
- Arkivit të Qeverisë