CONTENTS

(This Page Intentionally Left Blank)

PREFACE

On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD)–5, *Management of Domestic Incidents*, which directs the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). This system provides a consistent nationwide template to enable Federal, State, local, and tribal governments and private-sector and nongovernmental organizations to work together effectively and efficiently to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity, including acts of catastrophic terrorism. This document establishes the basic elements of the NIMS and provides mechanisms for the further development and refinement of supporting national standards, guidelines, protocols, systems, and technologies.

Building on the foundation provided by existing incident management and emergency response systems used by jurisdictions and functional disciplines at all levels, this document integrates best practices that have proven effective over the years into a comprehensive framework for use by incident management organizations in an all-hazards context (terrorist attacks, natural disasters, and other emergencies) nationwide. It also sets in motion the mechanisms necessary to leverage new technologies and adopt new approaches that will enable continuous refinement of the NIMS over time. This document was developed through a collaborative, intergovernmental partnership with significant input from the incident management functional disciplines, the private sector, and nongovernmental organizations.

The NIMS represents a core set of doctrine, concepts, principles, terminology, and organizational processes to enable effective, efficient, and collaborative incident management at all levels. It is not an operational incident management or resource allocation plan. To this end, HSPD-5 requires the Secretary of Homeland Security to develop a National Response Plan (NRP) that integrates Federal government domestic prevention, preparedness, response, and recovery plans into a single, all-disciplines, all-hazards plan. The NRP, using the comprehensive framework provided by the NIMS, will provide the structure and mechanisms for national-level policy and operational direction for Federal support to State, local, and tribal incident managers and for exercising direct Federal authorities and responsibilities as appropriate under the law.

HSPD-5 requires all Federal departments and agencies to adopt the NIMS and to use it in their individual domestic incident management and emergency prevention, preparedness, response, recovery, and mitigation programs and activities, as well as in support of all actions taken to assist State, local, or tribal entities. The directive also requires Federal departments and agencies to make adoption of the NIMS by State and local organizations a condition for Federal preparedness assistance (through grants, contracts, and other activities) beginning in FY 2005. Jurisdictional compliance with certain aspects of the NIMS will be possible in the short term, such as adopting the basic tenets of the Incident

Command System (ICS) identified in this document. Other aspects of the NIMS, however, will require additional development and refinement to enable compliance at a future date (e.g., data and communications systems interoperability). The Secretary of Homeland Security, through the NIMS Integration Center discussed in Chapter VII, will publish separately the standards, guidelines, and compliance protocols for determining whether a Federal, State, local, or tribal entity has adopted the aspects of the NIMS that are in place by October 1, 2004. The Secretary, through the NIMS Integration Center, will also publish, on an ongoing basis, additional standards, guidelines, and compliance protocols for the aspects of the NIMS not yet fully developed.

CHAPTER I

INTRODUCTION AND OVERVIEW

A. INTRODUCTION.

Since the September 11, 2001, attacks on the World Trade Center and the Pentagon, much has been done to improve prevention, preparedness, response, recovery, and mitigation capabilities and coordination processes across the country. A comprehensive national approach to incident management, applicable at all jurisdictional levels and across functional disciplines, would further improve the effectiveness of emergency response providers[1] and incident management organizations across a full spectrum of potential incidents and hazard scenarios. Such an approach would also improve coordination and cooperation between public and private entities in a variety of domestic incident management activities. For purposes of this document, incidents can include acts of terrorism, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, typhoons, war-related disasters, etc.

On February 28, 2003, the President issued Homeland Security Presidential Directive (HSPD)-5, which directs the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). According to HSPD-5:

> This system will provide a consistent nationwide approach for Federal, State,[2] and local[3] governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility

---

[1] As defined in the Homeland Security Act of 2002, Section 2(6), "The term 'emergency response providers' includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities." 6 U.S.C. 101(6)

[2] As defined in the Homeland Security Act of 2002, the term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States. 6 U.S.C. 101(14).

[3] As defined in the Homeland Security Act of 2002, Section 2(10), the term," local government" means "(A) county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity." 6 U.S.C. 101(10).

among Federal, State, and local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system; multiagency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certification; and the collection, tracking, and reporting of incident information and incident resources.

While most incidents are generally handled on a daily basis by a single jurisdiction at the local level, there are important instances in which successful domestic incident management operations depend on the involvement of multiple jurisdictions, functional agencies, and emergency responder disciplines. These instances require effective and efficient coordination across this broad spectrum of organizations and activities. The NIMS uses a systems approach to integrate the best of existing processes and methods into a unified national framework for incident management. 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 incident management operations. It does this through a core set of concepts, principles, procedures, organizational processes, terminology, and standards requirements applicable to a broad community of NIMS users.

B. CONCEPTS AND PRINCIPLES.

To provide this framework for interoperability and compatibility, the NIMS is based on an appropriate balance of flexibility and standardization.

1. Flexibility.

The NIMS provides a consistent, flexible, and adjustable national framework within which government and private entities at all levels can work together to manage domestic incidents, regardless of their cause, size, location, or complexity. This flexibility applies across all phases of incident management: prevention, preparedness, response, recovery, and mitigation.

2. Standardization.

The NIMS provides a set of standardized organizational structures—such as the Incident Command System (ICS), multiagency coordination systems, and public information systems—as well as requirements for processes, procedures, and systems designed to improve interoperability among jurisdictions and disciplines in various areas, including: training; resource management; personnel qualification and certification; equipment certification; communications and information management; technology support; and continuous system improvement.

C. OVERVIEW.

The NIMS integrates existing best practices into a consistent, nationwide approach to domestic incident management that is applicable at all jurisdictional levels and across functional disciplines in an all-hazards context. Six major components make up this systems approach. Each is addressed in a separate chapter of this document. Of these components, the concepts and practices for Command and Management (Chapter II) and Preparedness (Chapter III) are the most fully developed, reflecting their regular use by many jurisdictional levels and agencies responsible for incident management across the country. Chapters IV-VII, which cover Resource Management, Communications and Information Management, Supporting Technologies, and Ongoing Management and Maintenance, introduce many concepts and requirements that are also integral to the NIMS but that will require further collaborative development and refinement over time.

1. NIMS Components.

The following discussion provides a synopsis of each major component of the NIMS, as well as how these components work together as a system to provide the national framework for preparing for, preventing, responding to, and recovering from domestic incidents, regardless of cause, size, or complexity. A more detailed discussion of each component is included in subsequent chapters of this document.

a. Command and Management.

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

(1) The ICS.

The ICS defines the operating characteristics, interactive management components, and structure of incident management and emergency response organizations engaged throughout the life cycle of an incident;

(2) Multiagency Coordination Systems.

These define the operating characteristics, interactive management components, and organizational structure of supporting incident management entities engaged at the Federal, State, local, tribal, and regional levels through mutual-aid agreements and other assistance arrangements; and

(3) Public Information Systems.

These refer to processes, procedures, and systems for communicating timely and accurate information to the public during crisis or emergency situations.

b. Preparedness.

Effective incident management begins with a host of preparedness activities conducted on a "steady-state" basis, well in advance of any potential incident. Preparedness involves an integrated combination of planning, training, exercises, personnel qualification and certification standards, equipment acquisition and certification standards, and publication management processes and activities.

(1) Planning

Plans describe how personnel, equipment, and other resources are used to support incident management and emergency response activities. Plans provide mechanisms and systems for setting priorities, integrating multiple entities and functions, and ensuring that communications and other systems are available and integrated in support of a full spectrum of incident management requirements.

(2) Training

Training includes standard courses on multiagency incident command and management, organizational structure, and operational procedures; discipline-specific and agency-specific incident management courses; and courses on the integration and use of supporting technologies.

(3) Exercises

Incident management organizations and personnel must participate in realistic exercises—including multidisciplinary, multijurisdictional, and multisector interaction—to improve integration and interoperability and optimize resource utilization during incident operations.

(4) Personnel Qualification and Certification

Qualification and certification activities are undertaken to identify and publish national-level standards and measure performance against these standards to ensure that incident management and emergency responder personnel are appropriately qualified and officially certified to perform NIMS-related functions.

(5) Equipment Acquisition and Certification

Incident management organizations and emergency responders at all levels rely on various types of equipment to perform mission essential tasks. A critical component of operational preparedness is the acquisition of equipment that will perform to certain standards, including the capability to be interoperable with similar equipment used by other jurisdictions.

(6) Mutual Aid

Mutual-aid agreements are the means for one jurisdiction to provide resources, facilities, services, and other required support to another jurisdiction during an incident. Each jurisdiction should be party to a mutual-aid agreement with appropriate jurisdictions from which they expect to receive or to which they expect to provide assistance during an incident.

(7) Publications Management

Publications management refers to forms and forms standardization, developing publication materials, administering publications—including establishing naming and numbering conventions, managing the publication and promulgation of documents, and exercising control over sensitive documents—and revising publications when necessary.

c. Resource Management.

The NIMS defines standardized mechanisms and establishes requirements for processes to describe, inventory, mobilize, dispatch, track, and recover resources over the life cycle of an incident.

d. Communications and Information Management.

The NIMS identifies the requirement for a standardized framework for communications, information management (collection, analysis, and dissemination), and information-sharing at all levels of incident management. These elements are briefly described as follows:

(1) Incident Management Communications.

Incident management organizations must ensure that effective, interoperable communications processes, procedures, and systems exist to support a wide variety of incident management activities across agencies and jurisdictions.

(2) Information Management.

Information management processes, procedures, and systems help ensure that information, including communications and data, flows efficiently through a commonly accepted architecture supporting numerous agencies and jurisdictions responsible for managing or directing domestic incidents, those impacted by the incident, and those contributing resources to the incident management effort. Effective information management enhances incident management and response and helps insure that crisis decision-making is better informed.

e. Supporting Technologies.

Technology and technological systems provide supporting capabilities essential to implementing and continuously refining the NIMS. These include voice and data communications systems, information management systems (i.e., record keeping and resource tracking), and data display systems. Also included are specialized technologies that facilitate ongoing operations and incident management activities in situations that call for unique technology-based capabilities.

f. Ongoing Management and Maintenance.

This component establishes an activity to provide strategic direction for and oversight of the NIMS, supporting both routine review and the continuous refinement of the system and its components over the long term.

2. Appendices.

The appendices to this document provide additional system details regarding the ICS and resource typing.

CHAPTER II

COMMAND AND MANAGEMENT

This chapter describes the systems used to facilitate domestic incident command and management operations, including the ICS, multiagency coordination systems, and the Joint Information System (JIS). Additional details on incident command and management are contained in Appendix A.

A. INCIDENT COMMAND SYSTEM.

The ICS is a management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to enable effective and efficient domestic incident management. A basic premise of ICS is that it is widely applicable. It is used to organize both near-term and long-term field-level operations for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade. ICS is used by all levels of government—Federal, State, local, and tribal—as well as by many private-sector and nongovernmental organizations. ICS is also applicable across disciplines. It is normally structured to facilitate activities in five major functional areas: command, operations, planning, logistics, and finance and administration.

Acts of biological, chemical, radiological, and nuclear terrorism represent particular challenges for the traditional ICS structure. Events that are not site specific, are geographically dispersed, or evolve over longer periods of time will require extraordinary coordination between Federal, State, local, tribal, private-sector, and nongovernmental organizations. An area command may be established to oversee the management of such incidents. (See Appendix A, Tab 6.)

1. Concepts and Principles.

a. Most Incidents Are Managed Locally.

The initial response to most domestic incidents is typically handled by local "911" dispatch centers, emergency responders within a single jurisdiction, and direct supporters of emergency responders. Most responses need go no further. In other instances, incidents that begin with a single response discipline within a single jurisdiction may rapidly expand to multidiscipline, multijurisdictional incidents requiring significant additional resources and operational support. Whether for incidents in which additional resources are required or are provided from different organizations within a single jurisdiction or outside the

jurisdiction, or for complex incidents with national-level implications (such as an emerging infectious disease or a bioterror attack), the ICS provides a flexible core mechanism for coordinated and collaborative incident management. When a single incident covers a large geographical area, multiple local ICS organizations may be required. Effective cross-jurisdictional coordination using processes and systems described in the NIMS is absolutely critical in this instance.

b. The NIMS Requires That Field Command and Management Functions Be Performed in Accordance with a Standard Set of ICS Organizations, Doctrine, and Procedures.

However, Incident Commanders generally retain the flexibility to modify procedures or organizational structure to align as necessary with the operating characteristics of their specific jurisdictions or to accomplish the mission in the context of a particular hazard scenario.

c. ICS Is Modular and Scalable.

ICS is designed to have the following operating characteristics; it should be

- suitable for operations within a single jurisdiction or single agency, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement;
- applicable and acceptable to users throughout the country;
- readily adaptable to new technology;
- adaptable to any emergency or incident to which domestic incident management agencies would be expected to respond; and
- have a scalable organizational structure that is based on the size and complexity of the incident.

d. ICS Has Interactive Management Components.

These set the stage for effective and efficient incident management and emergency response.

e. ICS Establishes Common Terminology, Standards, and Procedures that Enable Diverse Organizations to Work Together Effectively.

These include a standard set of predesignated organizational elements and functions, common names for resources used to support incident operations, common “typing” for resources to reflect specific capabilities, and common identifiers for facilities and operational locations used to support incident operations.

f. ICS Incorporates Measurable Objectives.

Measurable objectives ensure fulfillment of incident management goals. Objective-setting begins at the top and is communicated throughout the entire organization.

g. The Implementation of ICS Should Have the Least Possible Disruption On Existing Systems and Processes

This will facilitate its acceptance across a nationwide user community and to insure continuity in the transition process from normal operations.

h. ICS Should Be User Friendly and Be Applicable Across a Wide Spectrum of Emergency Response and Incident Management Disciplines

This will enable the communication, coordination, and integration critical to an effective and efficient NIMS**.**

2. Management Characteristics.

ICS is based on proven management characteristics. Each contributes to the strength and efficiency of the overall system.

a. Common Terminology.

ICS establishes common terminology that allows diverse incident management and support entities 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 domestic incident management responsibilities are named and defined. Terminology for the organizational elements involved is standard and consistent.

(2) Resource Descriptions.

Major resources—including personnel, facilities, and major equipment and supply items—used to support incident management activities are given common names and are “typed” with respect to their capabilities, to help avoid confusion and to enhance interoperability. The process for accomplishing this task is specified in Chapter IV.

(3) Incident Facilities.

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

b. Modular Organization.

The incident command organizational structure develops in a top-down, modular fashion that is 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 the Incident Commander (IC), who bases these 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 positions expands to adequately address the requirements of the incident.

c. Management by Objectives.

Management by objectives represents an approach that is communicated throughout the entire ICS organization. This approach includes the following:

- establishing overarching objectives;
- developing and issuing assignments, plans, procedures, and protocols;
- establishing specific, measurable objectives for various incident management functional activities, and directing efforts to attain them, in support of defined strategic objectives; and
- documenting results to measure performance and facilitate corrective action.

d. Reliance on an Incident Action Plan.

Incident action plans (IAPs) provide a coherent means of communicating the overall incident objectives in the contexts of both operational and support activities.

e. Manageable Span of Control.

Span of control is key to effective and efficient incident management. Within ICS, the span of control of any individual with incident management supervisory responsibility should range from three to seven subordinates. 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. Predesignated Incident Locations and Facilities.

Various types of operational locations and support facilities are established in the vicinity of an incident to accomplish a variety of purposes, such as decontamination, donated goods processing, mass care, and evacuation. The IC will direct the identification and location of facilities based on the requirements of the situation at hand. Typical predesignated facilities include incident

command posts, bases, camps, staging areas, mass casualty triage areas, and others, as required. For a more complete discussion of predesignated locations and facilities, see Appendix A, Tab 7.

g. Comprehensive Resource Management.

Maintaining an accurate and up-to-date picture of resource utilization is a critical component of domestic incident management. Resource management includes processes for categorizing, ordering, dispatching, tracking, and recovering resources. It also includes processes for reimbursement for resources, as appropriate. Resources are defined as personnel, teams, equipment, supplies, and facilities available or potentially available for assignment or allocation in support of incident management and emergency response activities.

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 enable common situational awareness and interaction. Preparedness planning must address the equipment, systems, and protocols necessary to achieve integrated voice and data incident management 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 every individual has 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 control 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 at all jurisdictional levels and within individual functional areas during incident operations is essential. To that end, the following principles must be adhered to:

(1) Check-In.

All responders, regardless of agency affiliation, must report in to receive an assignment in accordance with the procedures established by the IC.

(2) Incident Action Plan.

Response operations must be directed and coordinated as outlined in the IAP.

(3) Unity of Command.

Each individual involved in incident operations will be assigned to only one supervisor.

(4) Span of Control.

Supervisors must be able to adequately supervise and control their subordinates, as well as communicate with and manage all resources under their supervision.

(5) Resource Tracking.

Supervisors must record and report resource status changes as they occur.

m. Deployment.

Personnel and equipment should respond only when requested or when dispatched by an appropriate authority.

n. Information and Intelligence Management.

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

3. ICS Organization and Operations.

a. Command and General Staff Overview.

The ICS organization has five major functions, as described in Figure 1. These are: command, operations, planning, logistics, and finance and administration (with a potential sixth functional area to cover the intelligence function, as described in paragraph 2.n. above).

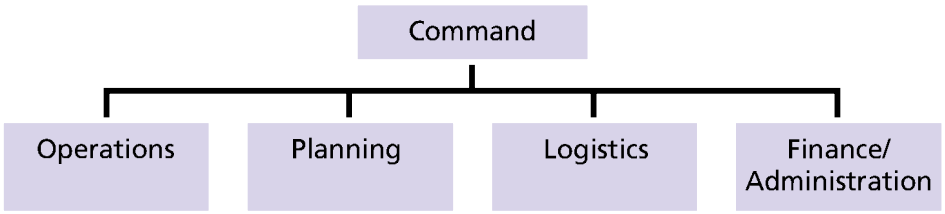

Figure 1—Incident Command System: Command Staff and General Staff

(1) Command.

Command comprises the IC and Command Staff. Command Staff positions are established to assign responsibility for key activities not specifically identified in the General Staff functional elements. These positions may include the Public Information Officer (PIO), Safety Officer (SO), and Liaison Officer (LNO), in addition to various others, as required and assigned by the IC.

(2) General Staff.

The General Staff comprises incident management personnel who represent the major functional elements of the ICS including the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief. (More detailed information regarding these functional elements is contained in Appendix A.) Command Staff and General Staff must continually interact and share vital information and estimates of the current and future situation and develop recommended courses of action for consideration by the IC. Additional information on the specific functions and makeup of the individual units within each of these sections is provided in Appendix A.

b. The Command Staff.

Command Staff is responsible for overall management of the incident. This includes Command Staff assignments required to support the command function.

(1) The Command Function.

The command function may be conducted in two general ways:

(a) Single Command IC.

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 in which incident

management crosses jurisdictional and/or functional agency boundaries, a single IC may be designated if all parties agree to such an option.) Jurisdictions should consider predesignating ICs in their preparedness plans.

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

(b) Unified Command.

UC is an important element in multijurisdictional or multiagency domestic 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 overcomes much of the inefficiency and duplication of effort that can occur when agencies from different functional and geographic jurisdictions, or agencies at different levels of government, operate without a common system or organizational framework. All agencies with jurisdictional authority or functional responsibility for any or all aspects of an incident and those able to provide specific resource support participate in the UC structure and contribute to the process of determining overall incident strategies; selecting objectives; ensuring that joint planning for tactical activities is accomplished in accordance with approved incident objectives; ensuring the integration of tactical operations; and 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 administrative jurisdictions are involved) and the type of incident (i.e., which functional agencies of the involved jurisdiction(s) are required). In the case of some multijurisdictional incidents, the designation of a single IC may be considered to promote greater unity of effort and efficiency.

(i) The designated agency officials participating in the UC represent different legal authorities and functional areas of responsibility and use a collaborative process to establish incident objectives and designate priorities that accommodate those objectives. Agencies heavily involved in the incident that lack jurisdictional responsibility are defined as supporting 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

Advantages of Using Unified Command

- A single set of objectives is developed for the entire incident
- A collective approach is used to develop strategies to achieve incident objectives
- Information flow and coordination is improved between all jurisdictions and agencies involved in the incident
- All agencies with responsibility for the incident have an understanding of joint priorities and restrictions
- No agency's legal authorities will be compromised or neglected
- The combined efforts of all agencies are optimized as they perform their respective assignments under a single Incident Action Plan

officials are consolidated into a single planning process (discussed more fully in Appendix A, Tab 8), including

- responsibilities for incident management;
- incident objectives;
- resource availability and capabilities;
- limitations; and
- areas of agreement and disagreement between agency officials.

(ii) Incidents are managed under a single, collaborative approach, including the following:

- common organizational structure;
- single incident command post;
- unified planning process; and
- unified resource management.

(iii) Under UC, the IAP is developed by the Planning Section Chief 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 normally come from the agency with the greatest jurisdictional involvement. UC participants will agree on the designation of the Operations Section Chief.

(iv) UC works best when the participating members of the UC collocate at the Incident Command Post 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;
- Coordinate to establish a single system for ordering resources;
- Develop a consolidated IAP, written or oral, evaluated and updated at regular intervals; and
- Establish procedures for joint decision-making and documentation.

(v) The primary differences between the single command structure and the UC structure are that

- In a single command structure, the IC is solely responsible (within the confines of his or her authority) for establishing incident management objectives and strategies. The IC is directly responsible for ensuring that all functional area activities are directed toward accomplishment of the strategy.
- In a UC structure, the individuals designated by their jurisdictional authorities (or by departments within a single jurisdiction) must jointly determine objectives, strategies, plans, and priorities and work together to execute integrated incident operations and maximize the use of assigned resources.

(2) Command Staff Responsibilities.

In an incident command organization, the Command Staff consists of the Incident Command and various special staff positions. The special staff positions are specifically designated, report directly to the Incident Command, and are assigned responsibility for key activities that are not a part of the ICS General Staff functional elements. Three special staff positions are typically identified in ICS: Public Information Officer, Safety Officer, and Liaison Officer. 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.

(a) Public Information Officer.

The PIO is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements. The PIO develops accurate and complete information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external consumption. The PIO may also perform a key public information-monitoring role. Whether the command structure is single or unified,

only one incident PIO should be designated. Assistants may be assigned from other agencies or departments involved. The IC must approve the release of all incident-related information.

(b) Safety Officer.

The SO monitors incident operations and advises the IC 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 or UC and supervisors at all levels of incident management. The SO is, in turn, responsible to the IC for the set of systems and procedures necessary to ensure ongoing assessment of hazardous environments, coordination of multiagency safety efforts, and implementation of measures to promote emergency responder safety, as well as the general safety of incident operations. The SO has emergency authority to stop and/or prevent unsafe acts during incident operations. In a UC structure, a single SO should be designated, in spite of the fact that multiple jurisdictions and/or functional agencies may be involved. Assistants may be required and may be assigned from other agencies or departments constituting the UC. The SO, Operations Section Chief, and Planning Section Chief must coordinate closely regarding operational safety and emergency responder health and safety issues. The SO must also ensure the coordination of safety management functions and issues across jurisdictions, across functional agencies, and with private-sector and nongovernmental organizations. 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 entity contributes to the overall effort to protect all responder personnel involved in incident operations.

(c) Liaison Officer.

The LNO is the point of contact for representatives of other governmental agencies, nongovernmental organizations, and/or private entities. In either a single or UC structure, representatives from assisting or cooperating agencies and organizations coordinate through the LNO. Agency and/or organizational representatives assigned to an incident must have the authority to speak for their parent agencies and/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 LNO to facilitate coordination.

(d) Assistants.

In the context of large or complex incidents, Command Staff members may need one or more assistants to help manage their workloads. Each Command Staff member is responsible for organizing his or her assistants for maximum efficiency.

(e) Additional Command Staff.

Additional Command Staff positions may also be necessary depending on the nature and location(s) of the incident, and/or specific requirements established by the IC. For example, a Legal Counsel may be assigned directly to the Command Staff to advise the IC on legal matters, such as emergency proclamations, legality of evacuation orders, and legal rights and restrictions pertaining to media access. Similarly, a Medical Advisor may be designated and assigned directly to the Command Staff to provide advice and recommendations to the IC in the context of incidents involving medical and mental health services, mass casualty, acute care, vector control, epidemiology, and/or mass prophylaxis considerations, particularly in the response to a bioterrorism event.

c. The General Staff.

The General Staff represents and is responsible for the functional aspects of the incident command structure. The General Staff typically consists of the Operations, Planning, Logistics, and Finance/Administration Sections, which are discussed below:

(1) Operations Section.

This section is responsible for all activities focused on reduction of the immediate hazard, saving lives and property, establishing situational control, and restoration of normal operations.

Figure 2 depicts the primary organizational structure template for an Operations Section. For a more detailed discussion of the Operations Section, see Appendix A, Tab 2. Further expansions of this basic structure will vary according to numerous considerations and operational factors. In some cases, the organizational structure will be determined by jurisdictional boundaries. In other cases, a strictly functional approach will be used. In still others, a mix of functional and geographical considerations may be appropriate. The ICS offers flexibility in determining the right structural approach for the specific circumstances of the incident at hand.

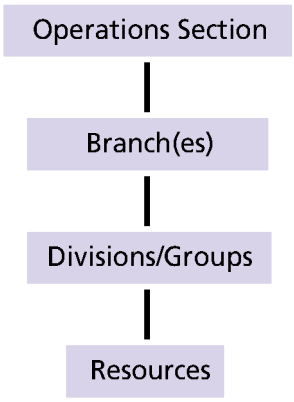

Figure 2—Major Organizational Elements of Operations Section

(a) Operations Section Chief.

The Operations Section Chief is responsible to the IC or UC for the direct management of all incident-related operational activities. The Operations Section Chief will establish tactical objectives for each operational period, with other section chiefs and unit leaders establishing their own supporting objectives. The Operations Section Chief may have one or more deputies assigned, with the assignment of deputies from other agencies encouraged in the case of multijurisdictional incidents. An Operations Section Chief should be designated for each operational period and should have direct involvement in the preparation of the IAP for the corresponding period of responsibility.

(b) Branches.

Branches may be used to serve several purposes, and may be functional or geographic in nature. In general, branches are established when the number of divisions or groups exceeds the recommended span of control of one supervisor to three to seven subordinates for the Operations Section Chief (a ratio of 1:5 is normally recommended, or 1:8 to 1:10 for many larger-scale law enforcement operations).

(c) Divisions and Groups.

Divisions and Groups are established when the number of resources exceeds the manageable span of control of the IC 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, the IC may assign intelligence-related activities to a functional group in the Operations Section. There also

may be additional levels of supervision below the Division or Group level.

(d) Resources.

Resources refer to the combination of personnel and equipment required to enable incident management operations. Resources may be organized and managed in three different ways, depending on the requirements of the incident:

(i) *Single Resources.* These are individual personnel and equipment items and the operators associated with them.

(ii) *Task Forces.* A Task Force is 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.

(iii) *Strike Teams.* Strike Teams are a set number of resources of the same kind and type that have an established minimum number of personnel. The use of Strike Teams and Task Forces is encouraged, wherever possible, 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.

(2) Planning Section.

The Planning Section collects, evaluates, and disseminates incident situation information and intelligence to the IC or UC and incident management personnel, prepares status reports, displays situation information, maintains status of resources assigned to the incident, and develops and documents the IAP based on guidance from the IC or UC. For a more detailed discussion of the Planning Section see Appendix A, Tab 3.

As shown in Figure 3, the Planning Section comprises 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.

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

The Planning Section is also responsible for developing and documenting the IAP. The IAP includes the overall incident objectives and strategies established by the IC or UC. In the case of 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

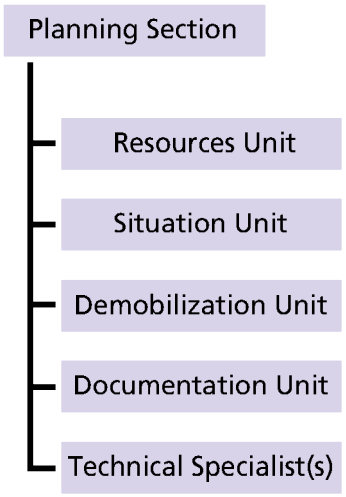

Figure 3—Planning Section Organization

organizations. The IAP also addresses tactical objectives and support activities required for one operational period, generally 12 to 24 hours. The IAP also contains provisions for continuous incorporation of "lessons learned" as incident management activities progress. An IAP is especially important when

(a) resources from multiple agencies and/or jurisdictions are involved;

(b) multiple jurisdictions are involved;

(d) the incident will effectively span several operational periods;

(d) changes in shifts of personnel and/or equipment are required; or

(e) there is a need to document actions and/or decisions.

The IAP will typically contain a number of components, as shown in Figure 4.[4]

[4] For full descriptions of units in each ICS section, see the tabs in Appendix A.

Components	Normally Prepared By
Common Components	
Incident Objectives	Incident Commander
Organization List or Chart	Resources Unit
Assignment List	Resources Unit
Communications Plan	Communications Unit
Logistics Plan	Logistics Unit
Responder Medical Plan	Medical Unit
Incident Map	Situation Unit
Health and Safety Plan	Safety Officer
Other Potential Components (Scenario 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
Operational Medical Plan	Technical Specialist
Evacuation Plan	Technical Specialist
Site Security Plan	Law Enforcement Specialist
Investigative Plan	Law Enforcement Specialist
Evidence Recovery Plan	Law Enforcement Specialist
Other	As Required

Figure 4—Sample IAP Outline

(3) Logistics Section.

The Logistics Section (Figure 5) is responsible for all support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. It also provides facilities, transportation, supplies, equipment maintenance and fuel, food services, communications and information technology support, and emergency responder medical services, including inoculations, as required. For a more detailed discussion of the Logistics Section see Appendix A, Tab 4.

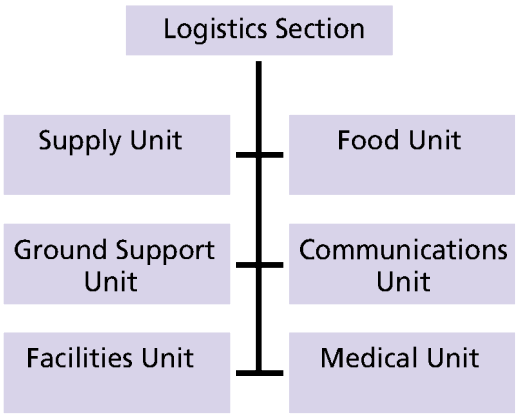

Figure 5—Logistics Section Organization

(4) Finance/Administration Section.

A Finance/Administration Section is established when the agency(s) involved in incident management activities require(s) finance and other administrative support services. Not all incidents will require a separate Finance/Administration Section. In cases that require only one specific function (e.g., cost analysis), this service may be provided by a technical specialist in the Planning Section. The basic organizational structure for a Finance/Administration Section is shown in Figure 6. When such a section is established, the depicted units may be created, as required. Appendix A, Tab 5, provides additional information relative to the function and responsibilities of each unit in this section.

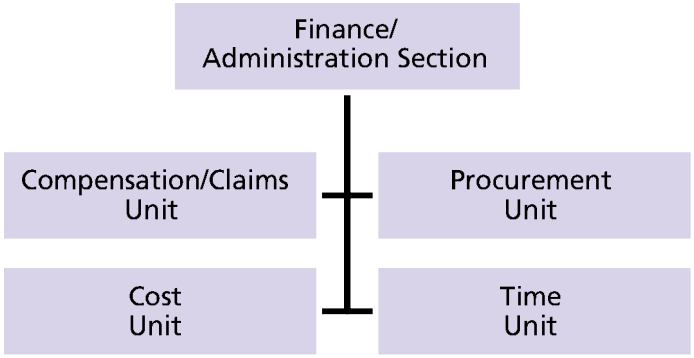

Figure 6—Finance and Administration Section Organization

(5) Information and Intelligence Function.

The analysis and sharing of information and intelligence are important elements of ICS. In this context, intelligence includes not only national

security or other types of classified information but also other operational information, such as risk assessments, medical intelligence (i.e., surveillance), weather information, geospatial data, structural designs, toxic contaminant levels, and utilities and public works data, that may come from a variety of different sources. Traditionally, information and intelligence functions are located in the Planning Section. However, in exceptional situations, the IC may need to assign the information and intelligence functions to other parts of the ICS organization. In any case, information and intelligence must be appropriately analyzed and shared with personnel, designated by the IC, who have proper clearance and a "need-to-know" to ensure that they support decision-making.

The intelligence and information function may be organized in one of the following ways:

(a) Within the Command Staff.

This option may be most appropriate in incidents with little need for tactical or classified intelligence and in which incident-related intelligence is provided by supporting Agency Representatives, through real-time reach-back capabilities.

(b) As a Unit Within the Planning Section.

This option may be most appropriate in an incident with some need for tactical intelligence and when no law enforcement entity is a member of the UC.

(c) As a Branch Within the Operations Section.

This option may be most appropriate in incidents with a high need for tactical intelligence (particularly classified intelligence) and when law enforcement is a member of the UC.

(d) As a Separate General Staff Section.

This option may be most appropriate when an incident is heavily influenced by intelligence factors or when there is a need to manage and/or analyze a large volume of classified or highly sensitive intelligence or information. This option is particularly relevant to a terrorism incident, for which intelligence plays a crucial role throughout the incident life cycle.

Regardless of how it is organized, the information and intelligence function is also responsible for developing, conducting, and managing information-related security plans and operations as directed by the IC. These can include information security and operational security activities, as well as the complex task of ensuring that sensitive information of all types (e.g., classified information, sensitive law enforcement information, proprietary

and personal information, or export-controlled information) is handled in a way that not only safeguards the information but also ensures that it gets to those who need access to it so that they can effectively and safely conduct their missions. The information and intelligence function also has the responsibility for coordinating information- and operational-security matters with public awareness activities that fall under the responsibility of the PIO, particularly where such public awareness activities may affect information or operations security.

4. Area Command.

a. Description.

An Area Command is activated only if necessary, depending on the complexity of the incident and incident management span-of-control considerations. An agency administrator or other public official with jurisdictional responsibility for the incident usually makes the decision to establish an Area Command. An Area Command is established either to oversee the management of multiple incidents that are each being handled by a separate ICS organization or to oversee the management of a very large incident that involves multiple ICS organizations, such as would likely be the case for incidents that are not site specific, geographically dispersed, or evolve over longer periods of time, (e.g., a bioterrorism event). In this sense, acts of biological, chemical, radiological, and/or nuclear terrorism represent particular challenges for the traditional ICS structure and will require extraordinary coordination between Federal, State, local, tribal, private-sector, and nongovernmental organizations. Area Command is also used when there are a number of incidents in the same area and of the same type, such as two or more hazardous material (HAZMAT) or oil spills, and fires. These represent incidents that may compete for the same resources. When incidents do not have similar resource demands, they are usually handled separately and are coordinated through an Emergency Operations Center (EOC). If the incidents under the authority of the Area Command are multijurisdictional, then a Unified Area Command should be established. This allows each jurisdiction to have representation in the command structure. Area Command should not be confused with the functions performed by an EOC. An Area Command oversees management of the incident(s), while an EOC coordinates support functions and provides resources support. (See Section B.2.a. below for further discussion of the EOC.)

b. Responsibilities.

For incidents under its authority, an Area Command has the responsibility to

- set overall incident-related priorities;
- allocate critical resources according to priorities;
- ensure that incidents are properly managed;

- ensure that incident management objectives are met and do not conflict with each other or with agency policy;
- identify critical resource needs and report them to EOCs and/or multiagency coordination entities; and
- ensure that short-term emergency recovery is coordinated to assist in the transition to full recovery operations.

See Appendix A, Tab 6 for additional information and guidance on establishing Area Commands.

B. MULTIAGENCY COORDINATION SYSTEMS.

1. Definition.

A multiagency coordination system is a combination of facilities, equipment, personnel, procedures, and communications integrated into a common system with responsibility for coordinating and supporting domestic incident management activities. The primary functions of multiagency coordination systems are to support incident management policies and priorities, facilitate logistics support and resource tracking, inform resource allocation decisions using incident management priorities, coordinate incident related information, and coordinate interagency and intergovernmental issues regarding incident management policies, priorities, and strategies. Direct tactical and operational responsibility for conducting incident management activities rests with the Incident Command.

2. System Elements.

Multiagency coordination systems may contain EOCs and (in certain multijurisdictional or complex incident management situations) multiagency coordinating entities:

a. Emergency Operations Center.

For purposes of this document, EOCs represent the physical location at which the coordination of information and resources to support incident management activities normally takes place. The Incident Command Post (ICP) located at or in the immediate vicinity of an incident site, although primarily focused on the tactical on-scene response, may perform an EOC-like function in smaller-scale incidents or during the initial phase of the response to larger, more complex events. Standing EOCs, or those activated to support larger, more complex events, are typically established in a more central or permanently established facility; at a higher level of organization within a jurisdiction. EOCs are organized by major functional discipline (fire, law enforcement, medical services, and so on); by jurisdiction (city, county, region, and so on); or, more likely, by some combination thereof. Department Operations Centers (DOCs)

normally focus on internal agency incident management and response and are linked to and, in most cases, are physically represented in a higher level EOC. ICPs should also be linked to DOCs and EOCs to ensure effective and efficient incident management.

For complex incidents, 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 (representatives of health care facilities, prehospital emergency medical services, patient transportation systems, pharmaceutical repositories, laboratories, etc.).

EOCs may be permanent organizations and facilities or may be established to meet temporary, short-term needs. 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 the specific organizational structure used, EOCs should include the following core functions: coordination; communications; resource dispatch and tracking; and information collection, analysis, and dissemination. EOCs may also support multiagency coordination and joint information activities as discussed below.

On activation of a local EOC, communications and coordination must be established between the IC or UC and the EOC, when they are not collocated. 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 during incidents, 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. Such agreements are discussed in Chapter III.

b. Multiagency Coordination Entities.

When incidents cross disciplinary or jurisdictional boundaries or involve complex incident management scenarios, a multiagency coordination entity, such as an emergency management agency, may be used to facilitate incident management and policy coordination. The situation at hand and the needs of the jurisdictions involved will dictate how these multiagency coordination entities conduct their business, as well as how they are structured. Multiagency coordination entities typically consist of principals (or their designees) from organizations and agencies with direct incident management responsibility or with significant incident management support or resource responsibilities. These entities are sometimes referred to as crisis action teams, policy committees,

incident management groups, executive teams, or other similar terms.[5] In some instances, EOCs may serve a dual function as a multiagency coordination entity; in others, the preparedness organizations discussed in Chapter III may fulfill this role. Regardless of the term or organizational structure used, these entities typically provide strategic coordination during domestic incidents. If constituted separately, multiagency coordination entities, preparedness organizations, and EOCs must coordinate and communicate with one another to provide uniform and consistent guidance to incident management personnel.

Regardless of form or structure, the principal functions and responsibilities of multiagency coordination entities typically include the following:

- ensuring that each agency involved in incident management activities is providing appropriate situational awareness and resource status information;
- establishing priorities between incidents and/or Area Commands in concert with the IC or UC(s) involved;
- acquiring and allocating resources required by incident management personnel in concert with the priorities established by the IC or UC;
- anticipating and identifying future resource requirements;
- coordinating and resolving policy issues arising from the incident(s); and
- providing strategic coordination as required.

Following incidents, multiagency coordination entities are also typically responsible for ensuring that improvements in plans, procedures, communications, staffing, and other capabilities necessary for improved incident management are acted on. These improvements should also be coordinated with appropriate preparedness organizations (see Chapter III), if these organizations are constituted separately.

C. PUBLIC INFORMATION SYSTEMS.

Systems and protocols for communicating timely and accurate information to the public are critical during crisis or emergency situations. This section describes the principles, system components, and procedures needed to support effective emergency public information operations.

1. Public Information Principles.

a. The PIO Supports the Incident Command.

Under the ICS, the Public Information Officer (PIO) is a key staff member supporting the incident command structure. The PIO represents and advises the

[5] For example, the wildland fire community has such an entity, the Multiagency Coordination Group (MAC Group).

Incident Command on all public information matters relating to the management of the incident. The PIO handles media and public inquiries, emergency public information and warnings, rumor monitoring and response, media monitoring, and other functions required to coordinate, clear with appropriate authorities, and disseminate accurate and timely information related to the incident, particularly regarding information on public health and safety and protection. The PIO is also responsible for coordinating public information at or near the incident site and serving as the on-scene link to the Joint Information System (JIS). In a large-scale operation, the on-scene PIO serves as a field PIO with links to the Joint Information Center (JIC), which is typically collocated with the Federal, regional, State, local, or tribal EOC tasked with primary incident coordination responsibilities. The JIS provides the mechanism for integrating public information activities among JICs, across jurisdictions, and with private-sector and nongovernmental organizations.

b. Public Information Functions Must Be Coordinated and Integrated Across Jurisdictions and Across Functional Agencies; Among Federal, State, Local, and Tribal Partners; and with Private-Sector and Nongovernmental Organizations.

During emergencies, the public may receive information from a variety of sources. The JIC provides a location for organizations participating in the management of an incident to work together to ensure that timely, accurate, easy-to-understand, and consistent information is disseminated to the public. The JIC comprises representatives from each organization involved in the management of an incident. In large or complex incidents, particularly those involving complex medical and public health information requirements, JICs may be established at various levels of government. All JICs must communicate and coordinate with each other on an ongoing basis. Public awareness functions must also be coordinated with the information- and operational-security matters that are the responsibility of the information and intelligence function of the ICS, particularly when public awareness activities may affect information or operations security.

c. Organizations Participating in Incident Management Retain Their Independence.

ICs and multiagency coordination entities are responsible for establishing and overseeing JICs including processes for coordinating and clearing public communications. In the case of UC, 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 entity contributes to the overall unified message.

2. System Description and Components.

a. Joint Information System.

The JIS provides an organized, integrated, and coordinated mechanism to ensure the delivery of understandable, timely, accurate, and consistent information to the public in a crisis. It includes the plans, protocols, and structures used to provide information to the public during incident operations, and encompasses all public information operations related to an incident, including all Federal, State, local, tribal and private organization PIOs, staff, and JICs established to support an incident. Key elements include the following:

- interagency coordination and integration;
- developing and delivering coordinated messages;
- support for decision-makers; and
- flexibility, modularity, and adaptability.

b. Joint Information Center.

A JIC is a physical location where public affairs professionals from organizations involved in incident management activities can collocate to perform critical emergency information, crisis communications, and public-affairs functions. It is important for the JIC to have the most current and accurate information regarding incident management activities at all times. The JIC provides the organizational structure for coordinating and disseminating official information. JICs may be established at each level of incident management, as required. Note the following:

- The JIC must include representatives of each jurisdiction, agency, private-sector, and nongovernmental organization involved in incident management activities.
- A single JIC location is preferable, but the system should be flexible and adaptable enough to accommodate multiple JIC locations when the circumstances of an incident require. Multiple JICs may be needed for a complex incident spanning a wide geographic area or multiple jurisdictions.
- Each JIC must have procedures and protocols to communicate and coordinate effectively with other JICs, as well as with other appropriate components of the ICS organization.

An example of typical JIC organization is shown in Figure 7.

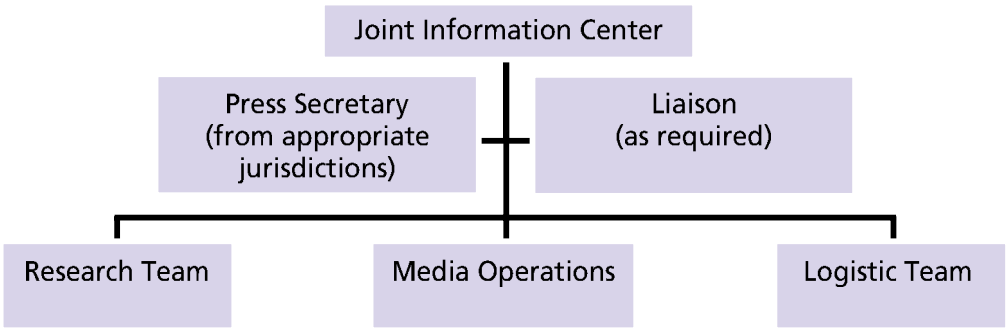

Figure 7—Joint Information Center Organization

(This Page Intentionally Left Blank)

CHAPTER III

PREPAREDNESS

This chapter describes specific measures and capabilities that jurisdictions and agencies should develop and incorporate into an overall system to enhance operational preparedness for incident management on a steady-state basis in an all-hazards context.[6] In developing, refining, and expanding preparedness programs and activities within their jurisdictions and organizations, incident management officials should leverage existing preparedness efforts and collaborative relationships to the greatest extent possible.

A. CONCEPTS AND PRINCIPLES.

Under the NIMS, preparedness is based on the following core concepts and principles:

1. Levels of Capability.

Preparedness involves actions to establish and sustain prescribed levels of capability necessary to execute a full range of incident management operations.

Preparedness is implemented through a continuous cycle of planning, training, equipping, exercising, evaluating, and taking action to correct and mitigate. Within the NIMS, preparedness focuses on guidelines, protocols, and standards for planning, training, personnel qualification and certification, equipment certification, and publication management.

2. A Unified Approach.

Preparedness requires a unified approach. A major objective of preparedness efforts is to ensure mission integration and interoperability in response to emergent crises across functional and jurisdictional lines, as well as between public and private organizations.

3. NIMS Publications.

The NIMS provides or establishes processes for providing guidelines; protocols; standards for planning, training, qualifications and certification; and publication

---

[6] The operational preparedness of our nation's incident management capabilities is distinct from the preparedness of individual citizens and private industry. Public preparedness for domestic incidents is beyond the scope of the NIMS but is an important element of homeland security.

management. National-level preparedness standards related to the NIMS will be maintained and managed through a multijurisdictional, multidiscipline center, using a collaborative process. (See Chapter VII.)

4. Mitigation.

Mitigation activities are important elements of preparedness and provide a critical foundation across the incident management spectrum from prevention through response and recovery.

Examples of key mitigation activities include the following:

- ongoing public education and outreach activities designed to reduce loss of life and destruction of property;
- structural retrofitting to deter or lessen the effects of incidents and reduce loss of life, destruction of property, and effects on the environment;
- code enforcement through such activities as zoning regulation, land management, and building codes; and
- flood insurance and the buy-out of properties subjected to frequent flooding, etc.

B. ACHIEVING PREPAREDNESS.

Individual Federal, State, local, and tribal jurisdictions are responsible for implementing the preparedness cycle in advance of an incident and appropriately including private-sector and nongovernmental organizations in such implementation. The NIMS provides the tools to ensure and enhance preparedness, as described in the sections that follow. These tools include preparedness organizations and preparedness programs that provide or establish processes for planning, training, and exercises; personnel qualification and certification; equipment certification; mutual aid; and publication management.

1. Preparedness Organizations.

Preparedness is the responsibility of individual jurisdictions; this responsibility includes coordinating various preparedness activities among all appropriate agencies within a jurisdiction, as well as across jurisdictions and with private organizations. This coordination is effected by mechanisms that range from individuals to small committees to large standing organizations. These mechanisms are referred to in this document as “preparedness organizations,” in that they serve as ongoing forums for coordinating preparedness activities in advance of an incident. Preparedness organizations represent a wide variety of committees, planning groups, and other organizations that meet regularly and coordinate with one another to ensure an appropriate focus on planning, training, equipping, and other preparedness requirements within a jurisdiction and/or across jurisdictions. The needs of the jurisdictions involved will dictate how frequently such organizations must conduct their business, as well as how they are structured. When preparedness activities

routinely need to be accomplished across jurisdictions, preparedness organizations should be multijurisdictional.. Preparedness organization at all jurisdictional levels should

- establish and coordinate emergency plans and protocols including public communications and awareness;
- integrate and coordinate the activities of the jurisdictions and functions within their purview;
- establish the standards, guidelines, and protocols necessary to promote interoperability among member jurisdictions and agencies;
- adopt standards, guidelines, and protocols for providing resources to requesting organizations, including protocols for incident support organizations;
- set priorities for resources and other requirements; and
- ensure the establishment and maintenance of multiagency coordination mechanisms, including EOCs, mutual-aid agreements, incident information systems, nongovernmental organization and private-sector outreach, public awareness and information systems, and mechanisms to deal with information and operations security.

2. Preparedness Programs.

Individual jurisdictions establish programs that address the requirements for each step of the preparedness cycle (planning, training, equipping, exercising, evaluating, and taking action to correct and mitigate). These programs should adopt relevant NIMS standards, guidelines, processes, and protocols.

a. Preparedness Planning.

Plans describe how personnel, equipment, and other governmental and nongovernmental resources will be used to support incident management requirements. Plans represent the operational core of preparedness and provide mechanisms for setting priorities, integrating multiple entities and functions, establishing collaborative relationships, and ensuring that communications and other systems effectively support the complete spectrum of incident management activities. The following are the principal types of plans:

(1) Emergency Operations Plan (EOP).

Each jurisdiction develops an EOP that defines the scope of preparedness and incident management activities necessary for that jurisdiction. The EOP should also describe organizational structures, roles and responsibilities, policies, and protocols for providing emergency support. The EOP facilitates response and short-term recovery activities (which set the stage for successful long-term recovery). It should drive decisions on long-term prevention and mitigation efforts or risk-based preparedness measures directed at specific hazards. An EOP should be flexible enough

for use in all emergencies. A complete EOP should describe the purpose of the plan, situation and assumptions, concept of operations, organization and assignment of responsibilities, administration and logistics, plan development and maintenance, and authorities and references. It should also contain functional annexes, hazard-specific appendices, and a glossary. EOPs should predesignate jurisdictional and/or functional area representatives to the IC or UC whenever possible to facilitate responsive and collaborative incident management. While the preparedness of the public is generally beyond the scope of the NIMS, EOPs should also include preincident and postincident public awareness, education, and communications plans and protocols.

(2) Procedures.

Each organization covered by the EOP should develop procedures that translate the tasking to that organization into specific action-oriented checklists for use during incident management operations, including how the organization will accomplish its assigned tasks. 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; mechanisms for reporting information to organizational work centers and EOCs; and communications operating instructions, including connectivity with private-sector and nongovernmental organizations. The development of procedures is required in accordance with the law for certain risk-based, hazard-specific programs. There are four standard levels of procedural documents:

- Overview—a brief concept summary of an incident-related function, team, or capability
- Standard Operating Procedure (SOP) or Operations Manual—a complete reference document that details the procedures for performing a single function or a number of interdependent functions
- Field Operations Guide (FOG) or Handbook—a durable pocket or desk guide that contains essential information required to perform specific assignments or functions.
- Job Aid—a checklist or other aid that is useful in performing or training for a job.

(3) Preparedness Plans.

Preparedness plans describe the process and schedule for identifying and meeting training needs (based on expectations the EOP has outlined); the process and schedule for developing, conducting, and evaluating exercises and correcting identified deficiencies; arrangements for procuring or

obtaining required incident management resources through mutual-aid mechanisms; and plans for facilities and equipment that can withstand the effects of hazards that the jurisdiction is more likely to face.

(4) Corrective Action and Mitigation Plans.

Corrective action plans are designed to implement procedures that are based on lessons learned from actual incidents or from training and exercises. Mitigation plans describe activities that can be taken prior to, during, or after an incident to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.

(5) Recovery Plans.

Recovery plans describe actions beyond rapid damage assessment and those necessary to provide immediate life support for victims. Long-term recovery planning involves identifying strategic priorities for restoration, improvement, and growth.

b. Training and Exercises.

Incident management organizations and personnel at all levels of government, and within the private-sector and nongovernmental organizations, must be appropriately trained to improve all-hazards incident management capability nationwide. Incident management organizations and personnel must also participate in realistic exercises—including multidisciplinary and multijurisdictional events and private-sector and nongovernmental organization interaction—to improve integration and interoperability. Training involving standard courses on incident command and management, incident management structure, operational coordination processes and systems—together with courses focused on discipline-specific and agency-specific subject-matter expertise—helps ensure that personnel at all jurisdictional levels and across disciplines can function effectively together during an incident.

To assist in this function, the NIMS Integration Center, as defined in Chapter VII, will

- Facilitate the development and dissemination 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 use of modeling and simulation capabilities for training and exercise programs.
- Facilitate the definition of general training requirements and approved training courses for all NIMS users. These requirements will be based on mission-to-task analysis. They will address critical elements of an effective national training system, including field-based training, specification of

mission-essential tasks, and requirements for specialized instruction. They will also cover fundamental administrative matters, such as instructor qualifications and course completion documentation.

- Review and approve (with the assistance of national professional organizations and with input from Federal, State, local, tribal, private-sector, and nongovernmental entities) discipline-specific requirements and training courses.

The training approach that has been developed for ICS serves as a model for course curricula and materials applicable to other components of the NIMS. ICS training is organized around four course levels: ICS-100, *Introduction to ICS*; ICS-200, *Basic ICS*; ICS-300, *Intermediate ICS*; and ICS-400 *Advanced ICS*. Course materials have been developed and shared by a number of Federal, State, local, tribal, and other specialized training providers in a nationally recognized effort. This allows use of a broad set of training providers and allows programs to be tailored to the specific circumstances that the Federal, State, local, and tribal levels face.

c. Personnel Qualification and Certification.

Under the NIMS, preparedness is based on national standards for the qualification and certification of emergency response personnel. Standards will help ensure that participating agencies and organizations field personnel who 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, currency, and physical and medical fitness. Personnel that are certified for employment in support of an incident that transcends interstate jurisdictions through the Emergency Management Assistance Compacts System will be required to meet national qualification and certification standards. Federal, State, local, and tribal certifying agencies; professional organizations; and private organizations should credential personnel for their respective jurisdictions.

To enable this qualification and certification function at the national level, the NIMS Integration Center, as defined in Chapter VII, will

- Facilitate the development and/or dissemination of national standards, guidelines, and protocols for qualification and certification.
- Review and approve (with the assistance of national professional organizations and with input from Federal, State, local, tribal, private-sector, and nongovernmental entities) the discipline-specific requirements submitted by functionally oriented incident management organizations and associations.
- Facilitate the establishment of a data maintenance system to provide incident managers with the detailed qualification, experience, and training

information needed to credential personnel for prescribed incident management positions.

d. Equipment Certification.

Incident management and emergency responder organizations at all levels rely on various types of equipment to perform mission essential tasks. A critical component of operational preparedness is the acquisition of equipment that will perform to certain standards, including the capability to be interoperable with equipment used by other jurisdictions.

To enable national-level equipment certification, the NIMS Integration Center, as defined in Chapter VII, will

- In coordination with appropriate Federal agencies, standards-making, certifying, and accrediting organizations and with appropriate State, local, tribal, private-sector, and nongovernmental organizations, facilitate the development and/or publication of national standards, guidelines, and protocols for equipment certification. This effort includes the incorporation of standards and certification programs already in use by incident management and emergency response organizations nationwide.
- Review and approve (with the assistance of national professional organizations and with input from Federal, State, local, tribal, and private-sector and nongovernmental entities) lists of emergency responder equipment that meet national certification requirements.

e. Mutual-Aid Agreements.

Mutual-aid agreements are the means for one jurisdiction to provide resources, facilities, services, and other required support to another jurisdiction during an incident. Each jurisdiction should be party to a mutual-aid agreement (such as the Emergency Management Assistance Compact) with appropriate jurisdictions from which they expect to receive or to which they expect to provide assistance during an incident. This would normally include all neighboring or nearby jurisdictions, as well as relevant private-sector and nongovernmental organizations. States should participate in interstate compacts and look to establish intrastate agreements that encompass all local jurisdictions. Mutual-aid agreements are also needed with private organizations, such as the American Red Cross, to facilitate the timely delivery of private assistance at the appropriate jurisdictional level during incidents.

At a minimum, mutual-aid agreements should include the following elements or provisions:

- definitions of key terms used in the agreement;
- roles and responsibilities of individual parties;
- procedures for requesting and providing assistance;

- procedures, authorities, and rules for payment, reimbursement, and allocation of costs;
- notification procedures;
- protocols for interoperable communications;
- relationships with other agreements among jurisdictions;
- workers compensation;
- treatment of liability and immunity;
- recognition of qualifications and certifications; and
- sharing agreements, as required.

Authorized officials from each of the participating jurisdictions will collectively approve all mutual-aid agreements.

f. Publication Management.

Publication management for the NIMS includes development of naming and numbering conventions; review and certification of publications; methods for publications control; identification of sources and suppliers for publications and related services; and management of publication distribution.

NIMS publication management includes the following types of products:

- qualifications information;
- training course and exercise information;
- task books;
- ICS training and forms;
- other necessary forms;
- job aids;
- guides;
- computer programs;
- audio and video resources;
- templates; and
- "best practices."

To enable national-level publication management, the NIMS Integration Center, as defined in Chapter VII, will

- Facilitate the development, publication, and dissemination of national standards, guidelines, and protocols for a NIMS publication management system.
- Facilitate the development of general publications for all NIMS users as well as their issuance via the NIMS publication management system.

- Review and approve (with the assistance of appropriate national professional standards-making, certifying, and accrediting organizations, and with input from Federal, State, local, tribal government and private-sector and nongovernmental organizations) the discipline-specific publication management requirements and training courses submitted by professional organizations and associations.

(This Page Intentionally Left Blank)

CHAPTER IV

RESOURCE MANAGEMENT

Resource management involves coordinating and overseeing the application of tools, processes, and systems that provide incident managers with timely and appropriate resources during an incident. Resources include personnel, teams, facilities, equipment, and supplies. Generally, resource management coordination activities take place within EOCs. When they are established, multiagency coordination entities may also prioritize and coordinate resource allocation and distribution during incidents.

Resource management involves four primary tasks:

- establishing systems for describing, inventorying, requesting, and tracking resources;
- activating these systems prior to and during an incident;
- dispatching resources prior to and during an incident; and
- deactivating or recalling resources during or after incidents.

The basic concepts and principles that guide the resource management processes used in the NIMS allow these tasks to be conducted effectively. By standardizing the procedures, methodologies, and functions involved in these processes, the NIMS ensures that resources move quickly and efficiently to support incident managers and emergency responders.

A. CONCEPTS AND PRINCIPLES.

1. Concepts.

The underlying concepts of resource management in this context are that

- It provides a uniform method of identifying, acquiring, allocating, and tracking resources.
- It uses effective mutual-aid and donor assistance and is enabled by the standardized classification of kinds and types of resources required to support the incident management organization.
- It uses a credentialing system tied to uniform training and certification standards to ensure that requested personnel resources are successfully integrated into ongoing incident operations.
- Its coordination is the responsibility of EOCs and/or multiagency coordination entities, as well as specific elements of the ICS structure (e.g., the Resources Unit discussed in detail in Appendix A, Tab 3–B).

- It should encompass resources contributed by private-sector and nongovernmental organizations.

2. Principles.

Five key principles underpin effective resource management:

a. Advance Planning.

Preparedness organizations (as defined in Section III.B.1) work together in advance of an incident to develop plans for managing and employing resources in a variety of possible emergency circumstances.

b. Resource Identification and Ordering.

Resource managers use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities. Resource managers perform these tasks either at an IC's request or in accordance with planning requirements.

c. Categorizing Resources.

Resources are categorized by size, capacity, capability, skill, and other characteristics. This makes the resource ordering and dispatch process within jurisdictions, across jurisdictions, and between governmental and nongovernmental entities more efficient and ensures that ICs receive resources appropriate to their needs. Facilitating the development and issuance of national standards for "typing" resources and "certifying" personnel will be the responsibility of the NIMS Integration Center described in Chapter VII.

d. Use of Agreements.

Preincident agreements among all parties providing or requesting resources are necessary to enable effective and efficient resource management during incident operations. Formal preincident agreements (e.g., mutual aid and the Emergency Management Assistance Compact [EMAC]) between parties, both governmental and nongovernmental, that might provide or request resources are established to ensure the employment of standardized, interoperable equipment, and other incident resources during incident operations.

e. Effective Management of Resources.

Resource managers use validated practices to perform key resource management tasks systematically and efficiently. Examples include the following:

(1) Acquisition Procedures.

Used to obtain resources to support operational requirements. Preparedness organizations develop tools and related standardized processes to support

acquisition activities. Examples include mission tasking, contracting, drawing from existing stocks, and making small purchases.

(2) Management Information Systems.

Used to collect, update, and process data; track resources; and display their readiness status. These tools enhance information flow and provide real-time data in a fast-paced environment where different jurisdictions and functional agencies managing different aspects of the incident life cycle must coordinate their efforts. Examples include geographical information systems (GISs), resource tracking systems, transportation tracking systems, inventory management systems, and reporting systems.

(3) Ordering, Mobilization, Dispatching, and Demobilization Protocols.

Used to request resources, prioritize requests, activate and dispatch resources to incidents, and return 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 performing the primary tasks of resource management, the NIMS includes standardized procedures, methodologies, and functions in its resource management processes. These processes reflect functional considerations, geographic factors, and validated practices within and across disciplines and are continually adjusted as new lessons are learned. The basic foundation for resource management provided in this chapter will be expanded and refined over time in a collaborative cross-jurisdictional, cross-disciplinary effort led by the NIMS Integration Center discussed in Chapter VII.

The NIMS uses eight processes for managing resources:

1. Identifying and Typing Resources.

Resource typing entails categorizing by capability the resources that incident managers commonly request, deploy, and employ. Measurable standards identifying the capabilities and performance levels of resources serve as the basis for categories. Resource users at all levels identify these standards and then type resources on a consensus basis, with a national-level entity taking the coordinating lead. Resource kinds may be divided into subcategories (types) to define more precisely the resource capabilities needed to meet specific requirements. Resource typing is a continuous process designed to be as simple as possible to facilitate frequent use and accuracy in obtaining needed resources. (See Appendix B for a more complete discussion of the NIMS national resource typing protocol.) To allow resources to be

deployed and used on a national basis, the NIMS Integration Center defined in Chapter VII is responsible for defining national resource typing standards.

2. Certifying and Credentialing Personnel.

Personnel certification entails authoritatively attesting that individuals meet professional standards for the training, experience, and performance required for key incident management functions. Credentialing involves providing documentation that can authenticate and verify the certification and identity of designated incident managers and emergency responders. This system helps ensure that personnel representing various jurisdictional levels and functional disciplines possess a minimum common level of training, currency, experience, physical and medical fitness, and capability for the incident management or emergency responder position they are tasked to fill.

3. Inventorying Resources.

Resource managers use various resource inventory systems to assess the availability of assets provided by public, private, and volunteer organizations. Preparedness organizations enter all resources available for deployment into resource tracking systems maintained at local, State, regional, and national levels. The data are then made available to 911 centers, EOCs, and multiagency coordination entities.

A key aspect of the inventorying process is determining whether or not the primary-use organization needs to warehouse items prior to an incident. Resource managers make this decision by considering the urgency of the need, whether there are sufficient quantities of required items on hand, and/or whether they can be produced quickly enough to meet demand. Another important part of the process is managing inventories with shelf-life or special maintenance considerations. Resource managers must build sufficient funding into their budgets for periodic replenishments, preventive maintenance, and capital improvements.

4. Identifying Resource Requirements.

Resource managers identify, refine, and validate resource requirements throughout the incident life cycle. This process involves accurately identifying (1) what and how much is needed, (2) where and when it is needed, and (3) who will be receiving or using it. Resources to be identified in this way include supplies, equipment, facilities, and incident management personnel and/or emergency response teams. If a requestor is unable to describe an item by resource type or classification system, resource managers provide technical advice to enable the requirements to be defined and translated into a specification.

Because resource availability and requirements will constantly change as the incident evolves, all entities participating in an operation must coordinate closely in this process. Coordination begins at the earliest possible point in the incident life cycle.

5. Ordering and Acquiring Resources.

Requests for items that the IC cannot obtain locally are submitted through the local EOC or multiagency coordinating entity using standardized resource-ordering procedures. If the servicing EOC is unable to fill the order locally, the order is forwarded to the next level—generally an adjacent local, State, regional EOC, or multiagency coordination entity.

6. Mobilizing Resources.

Incident 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 formally check in. This starts the on-scene in-processing and validates the order requirements. Notification that the resource has arrived is sent back through the system.

For resource managers, the mobilization process may include equipping, training, and/or inoculating personnel; 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.

EOCs and Incident Management Teams (IMTs) take direction from standard interagency mobilization guidelines at the national, regional, State, local, and tribal levels.

Managers should plan and prepare for the demobilization process well in advance, often at the same time they begin the resource mobilization process. Early planning for demobilization facilitates accountability and makes transportation of resources as efficient, costs as low, and delivery as fast as possible.

7. Tracking and Reporting Resources.

Resource tracking is a standardized, integrated process conducted throughout the life cycle of an incident by all agencies at all levels. This process provides incident managers with a clear picture of where resources are located, helps staff prepare to receive resources, protects the safety of personnel and security of supplies and equipment, and enables the coordination of movement of personnel, equipment, and supplies. Resource managers use established procedures to track resources continuously from mobilization through demobilization. Ideally, these managers would display this real-time information in a centralized database accessible to all NIMS partners, allowing total visibility of assets. Managers follow all required procedures for acquiring and managing resources, including reconciliation, accounting, auditing, and inventorying.

8. Recovering Resources.

Recovery involves the final disposition of all resources. During this process, resources are rehabilitated, replenished, disposed of, and retrograded:

a. Nonexpendable Resources.

These are fully accounted for at the incident site and again when they are returned to the unit that issued them. The issuing unit then restores the resources to fully functional capability and readies them for the next mobilization. Broken and/or lost items should be replaced through the Supply Unit, by the organization with invoicing responsibility for the incident, or as defined in preincident agreements. In the case of human resources, such as IMTs, adequate rest and recuperation time and facilities are provided. Mobilization guides developed at each jurisdictional level and within functional agencies provide appropriate rest and recuperation time guidelines. Important occupational health and mental health issues must also be addressed, including monitoring how such events affect emergency responders over time.

b. Expendable Resources.

These are also fully accounted for. Restocking occurs at the point from which a resource was issued. The incident management organization bears the costs of expendable resources, as authorized in preplanned financial agreements concluded by preparedness organizations. Returned resources that are not in restorable condition—whether expendable or nonexpendable—must be declared as excess according to established regulations and policies of the controlling entity. Waste management is of special note in the process of recovering resources. Resources that require special handling and disposition (e.g., biological waste and contaminated supplies, debris, and equipment) are dealt with according to established regulations and policies.

9. Reimbursement.

Reimbursement provides a mechanism to fund critical needs that arise from incident-specific activities. Reimbursement processes also play an important role in establishing and maintaining the readiness of resources. Processes and procedures must be in place to ensure that resource providers are reimbursed in a timely manner. These must include mechanisms for collecting bills, validating costs against the scope of the work, ensuring that proper authorities are involved, and accessing reimbursement programs, such as the Public Assistance Program and the Emergency Relief Program.

CHAPTER V

COMMUNICATIONS AND INFORMATION MANAGEMENT

Effective communications, information management, and information and intelligence sharing are critical aspects of domestic incident management. Establishing and maintaining a common operating picture and ensuring accessibility and interoperability are principal goals of communications and information management. A common operating picture and systems interoperability provide the framework necessary to

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

Prior to an incident, entities responsible for taking appropriate preincident actions use communications and information management processes and systems to inform and guide various critical activities. These actions include mobilization or predeployment of resources, as well as strategic planning by preparedness organizations, multiagency coordination entities, agency executives, jurisdictional authorities, and EOC personnel. During an incident, incident management personnel use communications and information processes and systems to inform the formulation, coordination, and execution of operational decisions and requests for assistance.

A. CONCEPTS AND PRINCIPLES.

1. A Common Operating Picture Accessible Across Jurisdictions and Functional Agencies.

A common operating picture allows incident managers at all levels to make effective, consistent, and timely decisions. Integrated systems for communication, information management, and intelligence and information sharing allow data to be continuously updated during an incident, providing a common framework that covers the incident's life cycle across jurisdictions and disciplines. A common operating picture helps ensure consistency at all levels of incident management across jurisdictions, as well as between various governmental jurisdictions and private-sector and nongovernmental entities that are engaged.

2. Common Communications and Data Standards.

Common communications and data standards and related testing and compliance mechanisms are fundamental to an effective NIMS. Communications interoperability in the context of incident management is also critical. Effective communications outside the incident structure—between other levels of government and between government and private entities—for resources and other support is also enhanced by adherence to such standards. Although much progress has been made in these areas, much more work remains to be done. Additional progress toward common communications and data standards and systems interoperability will be accomplished over time through a sustained collaborative effort facilitated by the NIMS Integration Center.

B. MANAGING COMMUNICATIONS AND INFORMATION.

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

1. Incident Management Communications.

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

a. Individual Jurisdictions.

These will be required to comply with national interoperable communications standards, once such standards are developed. Standards appropriate for NIMS users will be designated by the NIMS Integration Center in partnership with recognized standards development organizations (SDOs).

b. Incident Communications.

These will follow the standards called for under the ICS. The IC manages communications at an incident, using a common communications plan and an incident-based communications center established solely for use by the command, tactical, and support resources assigned to the incident. All entities involved in managing the incident will utilize common terminology, prescribed by the NIMS, for communications.

2. Information Management.

The NIMS Integration Center is charged with facilitating the definition and maintenance of the information framework required to guide the development of NIMS-related information systems. This framework consists of documented policies and interoperability standards.

a. Policies

(1) Preincident Information.

Preincident information needs are met at the Federal, State, local, and tribal levels, in concert with private-sector and nongovernmental organizations, primarily through the preparedness organizations described in Section III.B.1.

(2) Information Management.

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

(3) Networks.

Indications and warnings, incident notifications and public communications, and the critical information that constitute a common operating picture are disseminated through a combination of networks used by EOCs. Notifications are made to the appropriate jurisdictional levels and to private-sector and nongovernmental organizations through the mechanisms defined in emergency operations and incident action plans at all levels of government.

(4) Technology Use.

Agencies must plan in advance for the effective and efficient use of information management technologies (e.g., computers and networks) to tie together all command, tactical, and support units involved in incident management and to enable these entities to share information critical to mission execution and the cataloguing of required corrective actions.

b. Interoperability Standards.

Facilitating the development of data standards for the functions described below, including secure communications when required, is the responsibility of the NIMS Integration Center described in Chapter VII. Standards will be developed in accordance with the following design goals:

(1) Incident Notification and Situation Report.

Incident notification takes place at all levels. Although notification and situation report data must be standardized, it must not prevent information unique to a reporting organization from being collected or disseminated. Standardized transmission of data in a common format enables the passing of appropriate notification information to a national system that can handle data queries and information and intelligence assessments and analysis.

(2) Status Reporting.

All levels of government initiate status reports (e.g., Situation Reports [SITREPS] and Pollution Reports [POLREPS]) and then disseminate them to other jurisdictions. A standard set of data elements will be defined to facilitate this process.

(3) Analytical Data.

Analytical data, such as information on public health and environmental monitoring, is collected in the field in a manner that observes standard data definitions. It is then transmitted to laboratories using standardized analysis processes. During incidents that require public health and environmental sampling, multiple organizations at different levels of government often respond and collect data. Standardization of sampling and data collection enables more reliable laboratory analysis and improves the quality of assessments provided to decision-makers.

(4) Geospatial Information.

Geospatial information is used to integrate assessments, situation reports, and incident notification into a coherent common operating picture. Correct utilization of geospatial data is increasingly important to decision-makers. The use of geospatial data must be tied to consistent standards because of the potential for coordinates to be transformed incorrectly or otherwise misapplied, causing inconspicuous, yet serious, errors. Standards covering geospatial information should also be robust enough to enable systems to be used in remote field locations, where telecommunications capabilities may not have sufficient bandwidth to handle large images or are limited in terms of computing hardware.

(5) Wireless Communications.

To ensure that incident management organizations can communicate and share information with each other through wireless systems, the NIMS will include standards to help ensure that wireless communications and computing for Federal, State, local, and tribal public safety organizations and nongovernmental organizations are interoperable.

(6) Identification and Authentication.

Individuals and organizations that access the NIMS information management system and, in particular, those that 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 for the NIMS that is flexible and robust enough to ensure that information can be properly authenticated and protected. While the NIMS Integration Center is responsible for facilitating

the development of these standards, different levels of government and private organizations must collaborate to administer the authentication process.

(7) National Database of Incident Reports.

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

(This Page Intentionally Left Blank)

CHAPTER VI

SUPPORTING TECHNOLOGIES

Technology and technological systems provide supporting capabilities essential to implementing and continuously refining the NIMS. These include voice and data communications systems, information systems (i.e., record keeping and resource tracking), and display systems. These also include specialized technologies that facilitate incident operations and incident management activities in situations that call for unique technology-based capabilities.

Ongoing development of science and technology is integral to continual improvement and refinement of the NIMS. Strategic research and development (R&D) ensures that this development takes place. The NIMS also relies on scientifically based technical standards that support the nation's ability to prepare for, prevent, respond to, and recover from domestic incidents. Maintaining an appropriate focus on science and technology solutions as they relate to incident management will necessarily involve a long-term collaborative effort among NIMS partners.

A. CONCEPTS AND PRINCIPLES.

The NIMS leverages science and technology to improve capabilities and lower costs. It observes five key principles:

1. Interoperability and Compatibility.

Systems must be able to work together and should not interfere with one another if the multiple jurisdictions, organizations, and functions that come together under the NIMS are to be effective in domestic incident management. Interoperability and compatibility are achieved through the use of such tools as common communications and data standards, digital data formats, equipment standards, and design standards.

2. Technology Support.

Technology support permits organizations using the NIMS to enhance all aspects of incident management and emergency response. Technology support facilitates incident operations and sustains the research and development (R&D) programs that underpin the long-term investment in the nation's future incident management capabilities.

3. Technology Standards.

Supporting systems and technologies are based on requirements developed through preparedness organizations at various jurisdictional levels (see Section III.B.1). National standards for key systems may be required to facilitate the interoperability and compatibility of major systems across jurisdictional, geographic, and functional lines.

4. Broad-Based Requirements.

Needs for new technologies, procedures, protocols, and standards to facilitate incident management are identified at both the field and the national levels. Because these needs will most likely exceed available resources, the NIMS provides a mechanism for aggregating and prioritizing them from the local to the national level. These needs will be met across the incident life cycle by coordinating basic, applied, developmental, and demonstration research, testing, and evaluation activities.

5. Strategic Planning for R&D.

Strategic R&D planning identifies future technologies that can improve preparedness, prevention, response, and recovery capabilities or lower the cost of existing capabilities. To ensure effective R&D, the NIMS Integration Center, in coordination with the Under Secretary for Science and Technology of the Department of Homeland Security, will integrate into the national R&D agenda the incident management science and technology needs of departments, agencies, functional disciplines, private-sector entities, and nongovernmental organizations operating within the NIMS at the Federal, State, local, and tribal levels.

B. SUPPORTING INCIDENT MANAGEMENT WITH SCIENCE AND TECHNOLOGY.

Supporting technologies enhance incident management capabilities or lower costs through three principal activities: operational scientific support; technology standards support; and research and development support.

1. Operational Scientific Support.

Operational scientific support identifies and, on request, mobilizes scientific and technical assets that can be used to support incident management activities. Operational scientific support draws on the scientific and technological expertise of Federal agencies and other organizations. Planning for this category of support is done at each level of government through the NIMS preparedness organizations described in Section III.B.1. Operational scientific support is requisitioned and provided via the NIMS through various programs coordinated by the Department of Homeland Security and other organizations and agencies.

2. Technical Standards Support.

Technical standards support efforts enable the development and coordination of technology standards for the NIMS to ensure that personnel, organizations, communications and information systems, and other equipment perform consistently, effectively, and reliably together without disrupting one another. The NIMS Integration Center will coordinate the establishment of technical standards for NIMS users. The following principles will be used in defining these standards:

a. Performance Measurements as a Basis for Standards.

Performance measurement—collecting hard data on how things work in the real world—is the most reliable basis for standards that ensure the safety and mission effectiveness of emergency responders and incident managers. Within the technology standards process, a performance measurement infrastructure develops guidelines, performance standards, testing protocols, personnel certification, reassessment, and training procedures to help incident management organizations use equipment systems effectively.

b. Consensus-Based Performance Standards.

A consensus-based approach to standards builds on existing approaches to standards for interoperable equipment and systems and takes advantage of existing SDOs with long-standing interest and expertise. These SDOs include the National Institute of Justice, National Institute for Standards and Technology, National Institute for Occupational Safety and Health, American National Standards Institute, American Society for Testing and Materials, and National Fire Protection Association. The NIMS, through the NIMS Integration Center, establishes working relationships among these SDOs and incident management organizations at all levels to develop performance standards for incident management technology.

c. Test and Evaluation by Objective Experts.

NIMS technology criteria will rely on private- and public-sector testing laboratories to evaluate equipment against NIMS technical standards. These organizations will be selected in accordance with guidelines that ensure that testing organizations are both technically proficient and objective (free from conflicting interests) in their testing. The NIMS Integration Center will issue appropriate guidelines as part of its standards-development and facilitation responsibilities.

d. Technical Guidelines for Training Emergency Responders on Equipment Use.

Inputs from vulnerability analysts, equipment developers, users, and standards experts are employed to develop scientifically based technical guidelines for training emergency responders on how to use equipment properly. Based on

incident management protocols, instruments, and instrument systems, these training guidelines reflect threat and vulnerability information, equipment and systems capabilities, and a range of expected operating conditions. In addition, performance measures and testing protocols developed from these training guidelines provide a reproducible method of measuring the effectiveness of equipment and systems.

3. Research and Development to Solve Operational Problems.

R&D planning will be based on the operational needs of the entire range of NIMS users. These needs represent key inputs as the nation formulates its R&D agenda for developing new and improved incident management capabilities. Since operational needs will usually exceed the resources available for research to address them, these needs must be validated, integrated, and prioritized. The preparedness organizations described in Section III.B.1 perform these functions. The Department of Homeland Security is responsible for integrating user needs at all levels into the national R&D agenda.

CHAPTER VII

ONGOING MANAGEMENT AND MAINTENANCE

HSPD-5 requires the Secretary of Homeland Security to establish a mechanism for ensuring the ongoing management and maintenance of the NIMS. To this end, the Secretary will establish a multijurisdictional, multidisciplinary NIMS Integration Center. This center will provide strategic direction for and oversight of the NIMS, supporting both routine maintenance and continuous refinement of the system and its components over the long term. The center will include mechanisms for direct participation from and/or regular consultation with other Federal departments and agencies; State, local, and tribal incident management entities; emergency responder and incident management professional organizations; and private-sector and nongovernmental organizations.

The NIMS Integration Center will also be responsible for developing a process for ongoing revisions and updates to the NIMS. Revisions to the NIMS and other corrective actions can be proposed by

- local entities (including their preparedness organizations; see Chapter III);
- State entities (including their preparedness organizations; see Chapter III);
- regional entities (including their preparedness organizations; see Chapter III);
- tribal entities (including their preparedness organization; see Chapter III);
- Federal departments and agencies;
- private entities (including business and industry, volunteer organizations, academia, and other nonprofit and nongovernmental organizations); and
- NIMS-related professional associations.

A. CONCEPTS AND PRINCIPLES.

The process for managing and maintaining the NIMS ensures that all users and stakeholders—including various levels of government, functional disciplines, and private entities—are given the opportunity to participate in NIMS Integration Center activities. To accomplish this goal, the NIMS Integration Center will be multijurisdictional and multidisciplinary and will maintain appropriate liaison with private organizations.

The NIMS management and maintenance process relies heavily on lessons learned from actual incidents and domestic incident management training and exercises, as well as recognized best practices across jurisdictions and functional disciplines.

B. STRUCTURE AND PROCESS.

The Secretary of Homeland Security will establish and administer the NIMS Integration Center. Proposed changes to the NIMS will be submitted to the NIMS Integration Center for consideration, approval, and publication. The Secretary has ultimate authority and responsibility for publishing revisions and modifications to NIMS-related documents, including supplementary standards, procedures, and other materials, in coordination with other Federal, State, local, tribal, and private entities with incident management and emergency responder responsibilities, expertise, and experience.

C. RESPONSIBILITIES.

The NIMS Integration Center will be further responsible for

- developing a national program for NIMS education and awareness, including specific instruction on the purpose and content of this document and the NIMS in general;
- promoting compatibility between national-level standards for the NIMS and those developed by other public, private, and/or professional groups;
- facilitating the development and publication of materials (such as supplementary documentation and desk guides) and standardized templates to support implementation and continuous refinement of the NIMS;
- developing assessment criteria for the various components of the NIMS, as well as compliance requirements and compliance timelines for Federal, State, local, and tribal entities regarding NIMS standards and guidelines;
- facilitating the definition of general training requirements and the development of national-level training standards and course curricula associated with the NIMS, 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 NIMS users
  - the review and recommendation (in coordination with national professional organizations and Federal, State, local, tribal, private-sector, and nongovernmental entities) of discipline-specific NIMS training courses
- facilitating 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;
- facilitating the establishment and maintenance of a publication management system for documents supporting the NIMS and other NIMS-related publications and materials, including the development or coordination of general publications for all NIMS users, as well as their issuance via a NIMS publication management system;

- reviewing (in coordination with appropriate national professional standards-making, certifying, and accrediting organizations and with input from Federal, State, local, tribal, private-sector and nongovernmental entities) of the discipline-specific publication management requirements submitted by professional organizations and associations;
- facilitating the development and publication of national standards, guidelines, and protocols for the qualification and certification of emergency responder and incident management personnel, as appropriate;
- reviewing and approving (with the assistance of national professional organizations and with input from Federal, State, local, tribal, private-sector, and nongovernmental entities), as appropriate, the discipline-specific qualification and certification requirements submitted by emergency responder and incident management organizations and associations;
- facilitating the establishment and maintenance of a documentation and database system related to qualification, certification, and credentialing of incident management personnel and organizations, including reviewing and approving (in coordination with national professional organizations and with input from the Federal, State, local, tribal, private-sector and nongovernmental entities), as appropriate, of the discipline-specific requirements submitted by functionally oriented incident management organizations and associations.
- establishment of 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;
- coordination of minimum professional certification standards and facilitation of the design and implementation of a credentialing system that can be used nationwide;
- facilitating the establishment of standards for the performance, compatibility, and interoperability of incident management equipment and communications systems, including the following:
  - facilitating, in coordination with appropriate Federal agencies, standards-making, certifying, and accrediting organizations, and appropriate State, local, tribal, private-sector, and nongovernmental organizations, the development and/or publication of national standards, guidelines, and protocols for equipment certification (including the incorporation of standards and certification programs already in existence and used by incident management and emergency response organizations nationwide)
  - reviewing and approving (in coordination with national professional organizations and with input from Federal, State, local, tribal, private-sector, and nongovernmental entities) 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 the typing of resources;
- facilitating the definition and maintenance of the information framework required to guide the development of NIMS information systems, including the development of data standards for the following: incident notification and situation reports, status reporting, analytical data, geospatial information, wireless communications, identification and authentication, and incident reports, including "lessons learned" reports;
- coordinating the establishment of technical and technology standards for NIMS users in concert with the Under Secretary for Science and Technology of the Department of Homeland Security and recognized SDOs;
- integrating into the national R&D agenda, in coordination with the Under Secretary for Science and Technology of the Department of Homeland Security, the incident management science and technology needs of departments, agencies, disciplines, private-sector, and nongovernmental organizations operating within the NIMS at all levels; and
- establishing and maintaining a repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, as well as for best practices, model structures, and model processes for NIMS-related functions.