ORD 393 ~~M-05-002~~ PP-05-001

Shoreline City Clerk Receiving Number 3464

CITY OF SHORELINE
EMERGENCY OPERATIONS PLAN
BASIC PLAN

I. INTRODUCTION

A. Mission

It is the mission of the City of Shoreline to provide an emergency management organization and resources to minimize loss of life; protect property and natural resources; and restore the proper operation of the City in the event of a major natural or technological disaster.

B. Purpose

The purpose of this Plan is to establish policies and procedures that will enhance the ability of City government to restore its operations and to resume normal services during and after a disaster. The Plan identifies appropriate government response and recovery actions, and it identifies the resources that will be available to deal with a disaster.

C. Scope

This Plan applies to all personnel, offices, and functions of City government; to all volunteers who perform emergency management duties under City supervision; to appropriate contract services conducted in response to an emergency; and to all resources expended by the City in dealing with an emergency. The Plan will:

- Identify emergency response and recovery functions conducted by the City
- Identify departments responsible for those functions
- Establish fundamental policies, assumptions, and procedures
- Establish a coordinated concept of operations for City response and recovery
- Identify the relationship between the City of Shoreline, contract service providers, and other public or private agencies

D. Organization

Management of emergency response and recovery activities will be carried out by the elected and appointed officials of the City of Shoreline within the normal structure of city government. Contract services and our community partners will supplement and support City activities. This Plan is consistent with the *National Response Plan (NRP), the National Incident Management System (NIMS), Washington State Comprehensive Emergency Management Plan* and the *King County Regional Disaster Plan.*

This plan is based on the Incident Command System (ICS) as identified in the National Incident Management System (NIMS) and the Emergency Support Function (ESF) structure of federal, state and county emergency plans, adapted to Shoreline's needs. It consists of the following:

1. The **Basic Plan** describing the purpose, scope, situation, mission, policies, and concept of operations in an emergency.

2. **Emergency Support Functions (ESFs)** describe the purpose, planning assumptions, concept of operations, and responsibilities for the functions required in an emergency or disaster.

II. POLICIES

A. Authorities

This plan has been developed under the following local, state, and federal statutes and regulations:

- Shoreline Municipal Code 2.50
- King County Charter and County Code 1.28, 2.16, 2.56, 12.52;
- Revised Code of Washington 36.30, 38.52, 39.34;
- Washington Administrative Codes 118.04, 118.30, 296-62-3112;
- Public Law 92-288, The Disaster Relief Act of 1974, as amended;
- Public Law 920, Federal Civil Defense Act of 1950, as amended;
- Public Law 96-342, Improved Civil Defense Act of 1980;
- Title III, Superfund Amendments and Re-authorization Act of 1986 (Emergency Planning and Community Right-to-Know Act).

B. Assignment of Responsibilities

Basic responsibility for the protection of the health, safety and welfare of the individuals, families and general public within the boundaries of the City rests with the responsible officials of the City of Shoreline. When a disaster or emergency results in situations beyond the control or capability of those responsible officials, assistance may be requested of the next echelon of government.

City government has the primary responsibility for disaster mitigation, preparedness, response, and recovery for the City of Shoreline. The City will plan for disasters, direct operations, mobilize and control resources, and mitigate the impact of disasters on the City of Shoreline within the limits of available resources and capabilities.

Supplemental federal financial assistance would be available only when City, County, and State resources are not sufficient to cope with the situation and following a declaration by the President that the affected area was considered to be a "disaster area." Such Presidential declaration is made only following receipt of such a request from the governor. The governor will forward such a request, based on a like request received from appropriate authorities of the city and county affected, acknowledging that the resources of the affected area and the State are exhausted or inadequate to cope with the situation.

C. Limitations

No guarantee of a perfect response to disasters is expressed or implied by this Basic Plan or any parts or attachments. The City government assets and resources are vulnerable to disaster. In addition, the City is severely limited in the extent of its resources for coping with a major disaster. Fire, Police, and some public works services are provided by King County, by special purpose jurisdictions, or under contract. These services may be in short supply in a disaster, and State/federal assistance may be considerably delayed. The City will respond to the extent that it can given the situation, information, and resources available at the time.

III. SITUATION

A. Disaster Conditions and Hazards

The City is vulnerable to the effects of the forces of nature, including, but not limited to, flooding in the low lying areas of the City; severe storm; earthquake; fire; volcanic eruption; excessive precipitation causing landslides and overload of existing drainage systems; and high winds. In addition, other incidents such as nuclear incident or accident; aircraft accident; hazardous materials incidents or releases; train accident; and industrial accident or explosion could severely impact

the City. The City's location, topography, development history, future development plans, and resource base will all affect the degree to which the City remains or becomes vulnerable to disaster effects.

B. Planning Assumptions

- Priority of response will be for life safety, protection of public and private property, and natural resources, in that order.
- Disasters can occur at any time. Some emergencies or disasters will occur with sufficient warning to allow for appropriate warning and preparatory actions. Other disasters will provide no warning at all.
- The City will be unable to fulfill all emergency requests during a major disaster. Setting priorities for response will be necessary.
- All response resources will be overloaded, and a shortage of supplies will exist.
- Assistance from King County, Washington State, or the federal government will be delayed or not available for some time.
- The City, its citizens, and businesses should plan to be self-sufficient for at least 72 hours until emergency services can be restored. In some circumstances it may be much longer.
- People and organizations will adapt to the situation and will respond self-reliantly.
- Re-establishment of government functions and basic services will be critical to a speedy recovery after a disaster.
- The City will support employees' efforts to communicate with their families and to provide for their safety as necessary.

IV. CONCEPT OF OPERATIONS

A. General

City government, acting from the City Emergency Operations Center (EOC), is the focal point of the emergency management organization of the City of Shoreline. Mitigation and preparedness actions will be programmed and implemented by the elected and appointed officials of City government. During and after a disaster, the City emergency management organization will act from the Emergency Operations Center to mobilize and control City personnel and resources in dealing with and recovering from disaster effects.

B. Emergency Management Concepts

Protection of life, public and private property, the economy, and natural resources are the primary concerns of city government. Elected and appointed officials of the City will take all possible actions, within the limits of available resources, to mitigate the effects of a disaster and to assist response and recovery.

When a disaster occurs, all necessary steps will be taken by responsible officials to alleviate suffering and protect life and property. The cause and scope of the disaster will dictate the specific coordinated actions taken by those officials of the City with such responsibilities.

Normal organizational structures and reporting authority will be maintained to the extent possible.

Essential activities will be managed and directed from the EOC. Emergency operations may be conducted on a 24-hour basis.

If a situation is beyond the capabilities of the City, assistance will be requested through emergency services channels. Such requests will be prepared by the department or agency requiring assistance and coordinated with the Director of Emergency Management. The City will make maximum use of existing Mutual Aid Agreements.

City government will commit all available resources (materials, equipment, personnel, and supplies) prior to requesting additional aid from regional, state, or federal resources.

All emergency public information disseminated by the City of Shoreline will originate from the EOC and will be released only upon approval of the City Manager or a designated representative.

Services provided under contract will be coordinated with provider organizations and/or other jurisdictions through the EOC.

C. Direction and Control

The City Manager, or designee, is the Director of Emergency Management. The City Manager may designate an Emergency Management Coordinator and may delegate certain responsibilities to the Coordinator.

D. Emergency Operations Center (EOC)

The City Emergency Operations Center is located in the Shoreline Fire Training and Support Facility at 17525 Aurora Avenue North. The alternate EOC is at the Shoreline Police Station at 1206 North 185th Street.

During an EOC activation, access is limited to authorized personnel.

E. Phases of Emergency Management

1. Mitigation

Mitigation consists of actions taken prior to a disaster to prevent the occurrence of a disaster or to reduce the effects of a disaster should it occur. Mitigation actions taken by the City may include:

- Developing a mitigation plan to comply with Federal Emergency Management regulations
- Fostering public awareness of disaster effects
- Encouraging family and neighborhood preparedness programs
- Pursuing risk management and insurance programs
- Conducting structural and non-structural mitigation programs, where appropriate

2. Preparedness

Preparedness activities are necessary to the extent that mitigation measures cannot fully prevent disasters or eliminate their effects. Organizations develop plans and procedures to save lives and minimize damage by enhancing disaster response actions. Preparedness actions taken by the City may include:

- Developing emergency plans and procedures
- Conducting a Hazard Identification and Vulnerability Analysis
- Identifying resource needs
- Obtaining necessary resources and equipment, as appropriate
- Entering into inter-local agreements and contracts for emergency management assistance, as necessary
- Conducting emergency management training and exercises

3. Response

Response activities following a disaster include providing assistance for casualties, seeking to reduce the occurrence of secondary damage, and enhancing the speed of recovery operations. Response actions taken by the City may include:

- Warning and notification of City employees and residents
- Direction and control of City response operations
- Coordination of activities with King County and neighboring jurisdictions for resource augmentation and emergency assistance
- Provision of information and assistance to the public
- Damage assessment and reporting

4. Recovery

Recovery activities continue until all systems, facilities, and operations return to normal. Short-term recovery returns vital lifeline systems to minimum operating standards. Long-term recovery may continue for a number of years before life can return to normal, or better, levels. Recovery actions taken by the City, or coordinated through other public/private agencies, may include:

- Clearing debris
- Restoring City government operations and services
- Restoring basic lifeline systems (electric power, water, sewage, etc.)
- Participating in County and regional recovery activities
- Evaluating and modifying, as necessary, local zoning and building codes, development standards, permit requirements, etc.
- Updating hazard analyses, emergency plans and procedures

V. ADMINISTRATION AND LOGISTICS - RESPONSIBILITIES

A. City Council/Mayor

- Give advice and consent to the City Manager regarding emergency management policies and decisions.

- Adopt emergency management mutual aid plans and agreements and such ordinances, resolutions, rules and regulation as are necessary to implement emergency plans and agreements.

- Approve, at the earliest practical time after issuance, rules and regulations reasonably related to the protection of life and property, such rules and regulations having been made and issued by the Emergency Management Director.

- Approve mutual aid agreements as requested by the Emergency Management Director.

B. Director of Emergency Management/City Manager

- Serve as Chief Executive Officer of the City.

- Serve as the Director of Emergency Management.

- Proclaim local emergency

- Issue notice of evacuation when necessary.

- Appoint an Emergency Management Coordinator.

- Manage and administer City staff in their emergency management duties.

- Enforce and administer provisions, laws, and ordinances governing the City.

- Plan, coordinate, and direct the work of City departments in providing for preparedness needs, mitigation of, responding to and recovering from an emergency.

- Report to the City Council on general conditions, disaster circumstances, and the financial condition of the City.

- Advise the City Council regarding emergency policies for the City.

- Represent the City regarding the coordination of emergency response, mutual aid agreements, inter-local agreements, disaster recovery, etc.

- Oversee the development and implementation of continuity of government plans.

May amend the Plan as needed.

C. Deputy City Manager

- Assume the Duties of the City Manager in his/her absence.
- Serve as Public Information Officer/Liaison for the City during a disaster.
- Monitor disaster-related budget expenditures; oversee emergency contracting procedures.
- Assist in intergovernmental coordination of emergency response and recovery.
- Assist in recovery planning and operations.

D. Assistant City Manager

- Act as the King County Zone One coordinator.
- In the event the City Manager and Deputy City Manager are not available, assume the Duties of the City Manager as above.

E. Emergency Management Coordinator

- Provide expert technical assistance and information to the Director regarding emergency management, disaster response operations, and recovery.
- Assure that the Emergency Operations Plan and supporting procedures are reviewed and updated at least annually.
- Coordinate with King County and neighboring jurisdictions regarding emergency management and planning.
- Locate, configure, and equip an Emergency Operations Center.
- Develop procedures for activating, operating, and managing the EOC.
- Assist in developing and implementing a training program in emergency management tasks for City employees and volunteers.
- Ensure that all emergency management volunteers are registered by the City as emergency workers.
- Develop and conduct periodic emergency management exercises.

- Manage the operations of the EOC during a disaster.
- Prepare a post-disaster report and critique for the Director.
- Develop and coordinate a Neighborhood and Family Preparedness Program.
- Draft a Disaster Declaration for signature and promulgation by the City Manager.
- Chair the City's Emergency Management Council.
- Coordinate King County Regional Plan and Zone 1 activities.
- Act as liaison to enact the King County Regional Plan through Zone 1 coordinator.
- Coordinate mitigation and preparedness activities as appropriate.

F. City Clerk

- Serve as custodian of official records and perform official certification.
- Supervise Records Management Program for the City.
  1. Identify critical documents and essential records;
  2. Assist departments in identifying, managing, and storing essential records;
  3. Develop and implement a disaster recovery program for essential records.
- Oversee the preparation and publishing of official legal notices.
- Maintain City Council databases of ordinances, resolutions, minutes, policies, etc.

G. City Attorney

- Serve as chief legal advisor to the City.
- Provide legal advice to the City Council, City Manager, and department heads regarding emergency response and recovery operations.
- Issue legal opinions.

- Interpret laws, rulings, and regulations.
- Draft ordinances, resolutions, contracts, and other documents relating to emergency operations.

H. Communications and Inter-government Relations Director

- Assist the Public Information Officer in preparing and disseminating emergency public information.
- Assist in mobilizing and managing volunteers through the neighborhood associations.
- Assist in developing a Family and Neighborhood Preparedness Program.

I. Customer Response Team Supervisor

- Provide emergency response for routine City problems.
- Track customer requests and services on Hansen system.
- Coordinate with other departments for emergency/disaster services.
- Coordinate disaster information handling.

J. Financial Services Director

- Supervise the City's financial services staff.
- Oversee the central financial and management information system of the City.
- Manage and supervise the finance, accounting, and reporting operations of the City during a disaster, including all financial controls, audits, and reports. Ensure that proper documentation is maintained for all emergency-related expenditures.
- Supervise and direct the City's cash management functions; oversee the City's funds; maintain necessary banking relationships.
- Develop and implement emergency financial and procurement procedures as required. Coordinate with the City's bank and major vendors.
- Establish a unique project number for each disaster for all disaster-related expenses.

- Establish provisions for emergency signature authority for City checks during an emergency.
- Coordinate with the City's bank to establish emergency provisions for cash and lines of credit.
- Gather, interpret, and report information on emergency costs and expenditures.
- Prepare and report data for recovery of disaster relief funds.
- Project the costs of various disaster recovery options; prepare fiscal plans and projected budgets for disaster recovery.
- Maintain databases on emergency resource providers (equipment and material).
- Manage the City's Risk Management functions.

K. Human Resources Director

- Develop and implement personnel policies and procedures for emergency operations, to include any special considerations for those employees with disabilities.
- Maintain master personnel files, to include current employee emergency notification information that are accessible during an emergency, ensuring confidentiality of materials in accordance with state and federal laws.
- Register all emergency management volunteers as emergency workers.
- Plan to staff the Emergency Operations Center, as requested.
- Develop and implement an educational program in emergency management tasks for all City employees and volunteers.
- Develop a program to support the safety and well being of City employees' families during a disaster.

L. Human Services Manager

- Coordinate the implementation of social services programs, as appropriate, during emergency operations.
- Coordinate with social service organizations, relief agencies, the Red Cross, etc.

- Maintain liaison with organizations that outreach to at risk populations; the elderly, people with disabilities, and/or those who do not speak English to identify ways to meet their needs during an emergency.

M. Information Services Manager

- Develop and maintain a program for protection and recovery of the City's data processing resources during/after a disaster.
- Oversee the restoration of City data processing capabilities during a disaster.
- Provide software, hardware, maps, and administrative support for the Geographical Information System.
- Provide support to other departments in computer network coordination and administration and in software support.
- Ensure daily backup and secure storage of centrally-managed data.
- Control data security as defined in City policies.
- Provide computer assistance to City staff, network backup, and maintenance of the local area network.
- Oversee and support the City's voice, wireless, telephone, and audio-visual systems for emergency operations.

N. Police Chief

Police Services are provided under contract by the King County Sheriff's Office. Police functions and responsibilities include: (See ESF #6 Law Enforcement)

1. Law enforcement
2. Traffic and crowd control
3. Staging and perimeter security
4. Explosive ordinance disposal
5. Protection of critical facilities (including the EOC)
6. Evacuation management
7. Crime scene control

8. Mass care management

O. Fire Chief

Fire Services are provided by the Shoreline Fire Department. Fire functions and responsibilities include: (See ESF #5 Fire and Emergency Medical Services)

1. Fire prevention
2. Fire suppression
3. Emergency Medical Services
4. Emergency rescue
5. Damage assessment
6. Hazardous Materials preparedness and response
7. Evacuation management

P. Planning and Development Services Director

- Organize and carry out both short-term and long-range planning during emergency operations and recovery.
- Manage the gathering, analyzing, interpreting, and reporting of disaster-related information, including disaster damage, response capabilities, regional disaster conditions, etc.
- Ensure that City ordinances, codes, and regulations are followed as much as possible in disaster response and recovery; recommend necessary and appropriate revisions to meet disaster conditions.
- Ensure compliance with the Growth Management Act, zoning requirements, State Environmental Policy Act, and State Emergency Management requirements.
- Maintain and manage Planning and Development assets.
- Coordinate building and structural inspections for safety and habitability following a disaster. Close facilities or restrict occupancy/use as required.

- Coordinate inspections and recommendations with utility districts, FHA and other government entities. Provide enforcement of codes, occupancy policies, and other site safety and demolition as appropriate.

- Assist in damage assessment and reporting.

- Manage, coordinate, and perform inspections of residential and commercial buildings.

- Review building plans for code compliance and manage the inspection of construction activities.

- Manage and maintain the permit tracking and database system.

Q. Parks, Recreation, and Cultural Services Director

- Coordinate and manage the use of the community centers and other appropriate facilities as emergency shelters as necessary.

- Develop and maintain a database of emergency volunteer workers (individuals and groups); assist in registration and training of volunteers.

- Maintain and manage Parks assets.

- Identify parks and other open areas that could be used for emergency debris deposit sites.

- Assist in managing the activities of emergency volunteer workers during a disaster.

- Assist in the mobilization and management of emergency volunteers.

- Assist in the development and presentation of emergency volunteer training programs

- Assist in the development and presentation of neighborhood and family preparedness programs.

R. Public Works Director

- Maintain and manage Public Works' assets.

- Provide technical assistance to Emergency Management Leadership Team and City staff during disaster response and recovery operations.

- Oversee the operations of contractors, service providers, and emergency response agencies regarding public works projects and assets.

- Maintain master files of Public Works' projects, development construction records, street operations and maintenance, and other relevant documents.

- Advise the Director of Emergency Management regarding codes, policies, and procedures for any response or recovery activity involving City roads, rights-of-way, or facilities.

- Provide oversight for Public Works crews and other support agencies engaged in emergency response and recovery activities, including: repair of water mains, pumps, motors, valves, fire hydrants, storage tanks, etc.; operating and servicing heavy road and construction equipment and vehicles; cleaning and repairing ditches, culverts, and catch basins; traffic control; repairing streets; repairing traffic control signs; heavy equipment rescue, clearing ice, snow, or debris from streets.

- Assist in damage assessment and reporting.

- Provide periodic response and recovery work progress reports to the EOC.

- Provide on-site direction and guidance to City employees and emergency volunteer workers during emergency operations; inspect work in progress to ensure compliance with codes and safety practices.

- Maintain liaisons with all utility providers within the city to allow for ease of working relationships during emergency situations.

VI. ADMINISTRATION OF THE PLAN

A. Development

The Emergency Management Coordinator is responsible for the development of all aspects of the City of Shoreline Emergency Management Plan and for ensuring that the Plan is consistent an in compliance with the National Response Plan, the National Incident Management System (NIMS), State Emergency Management and King County Regional Disaster Plan. The Coordinator will assist City staff in preparing appropriate SOPs, action checklists, alert rosters, and other functional attachments to the Plan.

B. Maintenance

The Emergency Management Coordinator will review this Plan annually and update it to reflect any changes in organization, roles, and responsibilities;

facilities or resources; potential hazards. Lessons learned from actual activation of this Plan and/or from emergency management exercises will be incorporated into the structure and content of the Plan. The Emergency Management Coordinator will also ensure that all function-specific information is correct and current.

C. Legal Compliance

The Emergency Management Coordinator will submit the Plan to other agencies as required by law.

VII. TRAINING AND EXERCISES

A. General

Training and exercise programs in emergency management serve to enhance operational readiness by improving individual skills and by testing the emergency management organization, plans, and procedures. Training and exercising are the principal means of validating the City's capability to implement its emergency management plan and to perform to the standards set by the State of Washington and the Federal Emergency Management Agency.

B. Training

The City will provide training for all employees and emergency volunteers on a periodic basis covering the implementation of the Plan, emergency roles and responsibilities, recent changes in hazards and vulnerabilities, and emergency resource management. Whenever possible, the City will avail itself of emergency management training opportunities afforded by the King County Office of Emergency Management, Washington State Division of Emergency Management, the Federal Emergency Management Agency, and other training providers.

C. Exercise

The City will conduct an exercise of the emergency management organization every year to test emergency plans and procedures specified in this Plan, to identify shortfalls in resources, to incorporate changes in circumstances or procedures, and to test coordination capabilities with service providers and neighboring jurisdictions. The City will participate in King County or regional emergency management exercises when requested to do so. An actual local emergency declaration may serve as a test of the city's operational capabilities as outlined in WAC 118-3—060,8.

NATIONAL INCIDENT MANAGEMENT SYSTEM

March 1, 2004

Homeland Security

(This Page Intentionally Left Blank)

NATIONAL INCIDENT MANAGEMENT SYSTEM

March 1, 2004

Homeland Security

(This Page Intentionally Left Blank)

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

March 1, 2004

MEMORANDUM FOR: Cabinet Secretaries
Agency Directors
Members of Congress
Governors
Tribal Leaders
Mayors
County, Township, and Parish Officials
State Homeland Security Advisors
Homeland Security Advisory Council
State, Territorial, Local, and Tribal First Responders

FROM: Tom Ridge

SUBJECT: National Incident Management System

In Homeland Security Presidential Directive (HSPD)-5, *Management of Domestic Incidents*, the President directed me to develop, submit for review to the Homeland Security Council, and administer a National Incident Management System (NIMS). This system will provide a consistent nationwide approach for Federal, State, local, and tribal governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

The NIMS has undergone extensive vetting and coordination within the Federal family. The development process has also included extensive outreach to State, local, and tribal officials; to the emergency response community; and to the private sector. As a result, the NIMS incorporates the best-practices currently in use by incident managers at all levels. In addition, effective incident management in the homeland security environment we now face involves new concepts, processes, and protocols that will require additional development and refinement over time. The collective input and guidance from all of our homeland security partners has been, and will continue to be, vital to the further development of an effective and comprehensive NIMS.

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 those 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, tribal and local organizations a condition for Federal preparedness assistance beginning in FY 2005. 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 identified in this document. Other aspects of the NIMS, however, will require further development and refinement to enable compliance at future dates.

I ask for your continued cooperation and assistance as we further develop and implement the NIMS and the associated National Response Plan (NRP). I look forward to working with you as we continue our collective efforts to better secure the homeland and protect our citizens from both natural disasters and acts of terrorism.

(This Page Intentionally Left Blank)

CONTENTS

CONTENTS v

PREFACE ix

CHAPTER I—INTRODUCTION AND OVERVIEW 1

A. Introduction 1

B. Concepts and Principles 2

C. Overview 3

CHAPTER II—COMMAND AND MANAGEMENT 7

A. Incident Command System 7

B. Multiagency Coordination Systems 26

C. Public Information Systems 28

CHAPTER III—PREPAREDNESS 33

A. Concepts and Principles 33

B. Achieving Preparedness 34

CHAPTER IV—RESOURCE MANAGEMENT 43

A. Concepts and Principles 43

B. Managing Resources 45

CHAPTER V—COMMUNICATIONS AND INFORMATION MANAGEMENT 49

A. Concepts and Principles 49

B. Managing Communications and Information 50

CHAPTER VI—SUPPORTING TECHNOLOGIES 55

A. Concepts and Principles 55

B. Supporting Incident Management with Science and Technology 56

CHAPTER VII—ONGOING MANAGEMENT AND MAINTENANCE 59

A. Concepts and Principles. 59

B. Structure and Process 60

C. Responsibilities 60

APPENDIX A—THE INCIDENT COMMAND SYSTEM 63

TAB 1—ICS ORGANIZATION 65

A. Functional Structure 65

B. Modular Extension 65
TAB 2—THE OPERATIONS SECTION 67
A. Operations Section Chief 68
B. Divisions and Groups 68
C. Resource Organization 70
D. Branches 70
E. Air Operations Branch 72
TAB 3—THE PLANNING SECTION 75
A. Planning Section Chief 75
B. Resources Unit 76
C. Situation Unit 76
D. Documentation Unit 77
E. Demobilization Unit 77
F. Technical Specialists 77
TAB 4—THE LOGISTICS SECTION 81
A. Supply Unit 82
B. Facilities Unit 82
C. Ground Support Unit 82
D. Communications Unit 83
E. Food Unit 84
F. Medical Unit 85
TAB 5—THE FINANCE/ADMINISTRATION SECTION 87
A. Time Unit 88
B. Procurement Unit 88
C. Compensation and Claims Unit 88
D. Cost Unit 88
TAB 6—ESTABLISHING AN AREA COMMAND 91
A. Responsibilities 91
B. Organization 92
C. Location 93
D. Reporting Relationships 93
TAB 7—PREDESIGNATED FACILITIES AND AREAS 95
A. Incident Command Post 95
B. Incident Base 95

C. Camps 95
D. Mobilization and Staging Areas 95
TAB 8—THE PLANNING PROCESS 97
A. Overview 97
B. Responsibilities and Specific Planning Activities 99
TAB 9—EXAMPLES OF ICS FORMS 105
APPENDIX B—NATIONAL INCIDENT MANAGEMENT RESOURCE TYPING SYSTEM 121
A. Purpose 121
B. Responsiblities 121
C. Elements of the National Typing Protocol 121
D. Example of A Resource for which Typing has Been Completed 124
GLOSSARY OF KEY TERMS 127
ACRONYMS 139

(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).

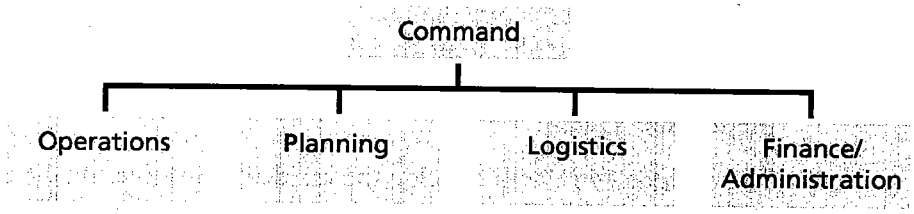

Figure 1—Incident Command System: Command Staff and General Staff

(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.

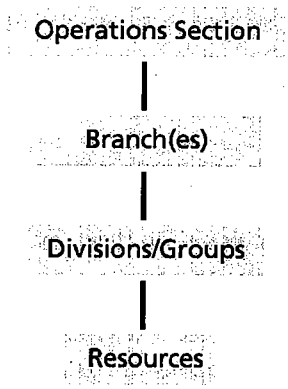

Figure 2—Major Organizational Elements of Operations Section

(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

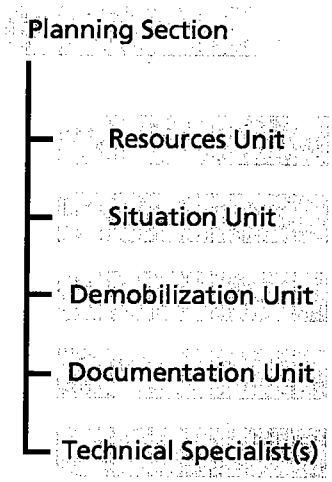

Figure 3—Planning Section Organization

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.

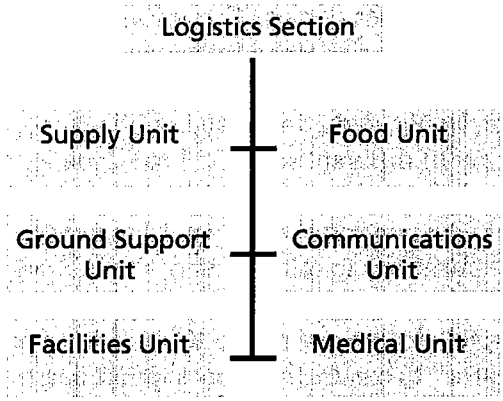

Figure 5—Logistics Section Organization

(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.

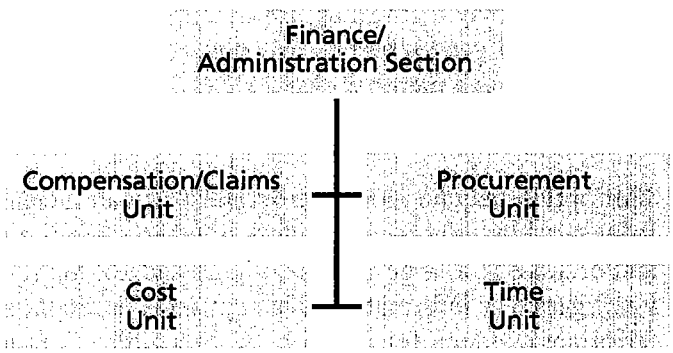

Figure 6—Finance and Administration Section Organization

(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.

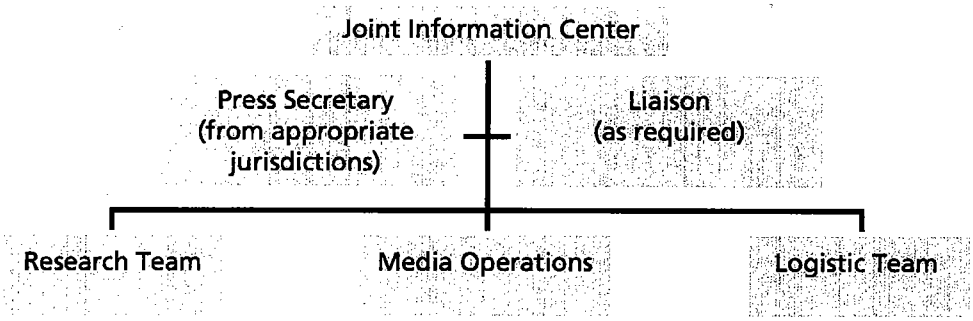

Figure 7—Joint Information Center Organization

(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.

APPENDIX A

THE INCIDENT COMMAND SYSTEM

The Incident Command System (ICS) is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in domestic incident management activities. It is used for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade, including acts of catastrophic terrorism. 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 usually organized around five major functional areas: command, operations, planning, logistics, and finance and administration. A sixth functional area, Intelligence, may be established if deemed necessary by the Incident Commander, depending on the requirements of the situation at hand.

Some of the more important "transitional steps" that are necessary to apply ICS in a field incident environment include the following:

- recognizing and anticipating the requirement that organizational elements will be activated and taking the necessary steps to delegate authority as appropriate;
- establishing incident facilities as needed, strategically located, to support field operations;
- establishing the use of common terminology for organizational functional elements, position titles, facilities, and resources; and
- rapidly evolving from providing oral direction to the development of a written Incident Action Plan.

(This Page Intentionally Left Blank)

TAB 1—ICS ORGANIZATION

A. FUNCTIONAL STRUCTURE.

The ICS organization comprises five major functional areas (Figure A-1): command, operations, planning, logistics, and finance and administration. (A sixth area, intelligence, may be established if required.)

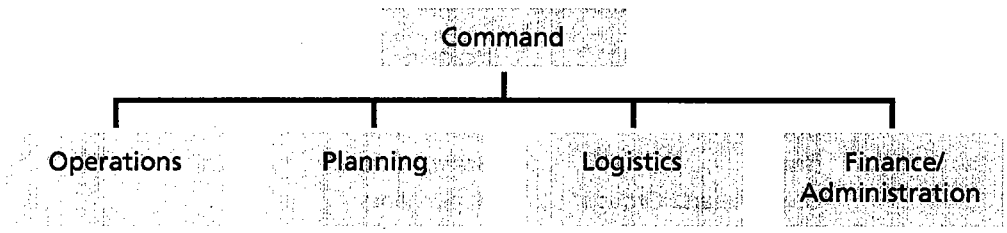

Figure A-1—Incident Command System: Basic Functional Structure

B. MODULAR EXTENSION.

The ICS organizational structure is modular, extending to incorporate all elements necessary for the type, size, scope, and complexity of a given incident. The IC structural organization builds from the top down; responsibility and performance begin with the incident command element and the IC. When the need arises, four separate sections can be used to organize the staff. Each of these may have several subordinate units, or branches, depending on the management requirements of the incident. If one individual can simultaneously manage all major functional areas, no further organization is required. If one or more of the functions requires independent management, an individual is assigned responsibility for that function.

The responding IC's initial management assignments will normally be one or more Section Chiefs to manage the major ICS functional areas (operations, planning, logistics, and finance and administration). The Section Chiefs will further delegate management authority for their areas as required. If a Section Chief sees the need, he or she may establish branches or units (depending on the section). Similarly, each functional unit leader will further assign individual tasks within the unit as needed.

The modular concept described above is based on the following considerations:

- developing the form of the organization to match the function or task to be performed;

- staffing only the functional elements that are required to perform the task;
- observing recommended span-of-control guidelines;
- performing the function of any nonactivated organizational element at the next highest level; and
- deactivating organizational elements no longer required.

For reference, Table A-1 describes the distinctive title assigned to each element of the ICS organization at each corresponding level, as well as the leadership title corresponding to each individual element.

Organizational Element	Leadership Position
Incident Command	Incident Commander (IC)
Command Staff	Officer
Section	Section Chief
Branch	Branch Director
Divisions and Groups*	Supervisors
Unit**	Unit Leader

*The hierarchical term *supervisor* is only used in the Operations Section.

**Unit leader designations apply to the subunits of the Planning, Logistics, and Finance/Administration Sections.

Table A-1—ICS Organization

TAB 2—THE OPERATIONS SECTION

The Operations Section is responsible for managing tactical operations at the incident site directed toward reducing the immediate hazard, saving lives and property, establishing situation control, and restoring normal conditions. Incidents can include acts of terrorism, wildland and urban fires, floods, hazardous material spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other incidents requiring an emergency response.

Because of its functional unit management structure, the ICS is applicable across a spectrum of incidents differing in size, scope, and complexity. The types of agencies that could be included in the Operations Section include fire, law enforcement, public health, public works, and emergency services, working together as a unit or in combinations, depending on the situation. Many incidents may involve private individuals, companies, or nongovernmental organizations, some of which may be fully trained and qualified to participate as partners in the Operations Section.

Incident operations can be organized and executed in many ways. The specific method selected will depend on the type of incident, agencies involved, and objectives and strategies of the incident management effort. The following discussion presents several different methods of organizing incident tactical operations. In some cases, a method will be selected to accommodate jurisdictional boundaries. In other cases, the approach will be strictly functional. In still others, a mix of functional and geographical approaches may be appropriate. The ICS offers extensive flexibility in determining the appropriate approach using the factors described above. Figure 2-A shows the primary organizational structure within the Operations Section.

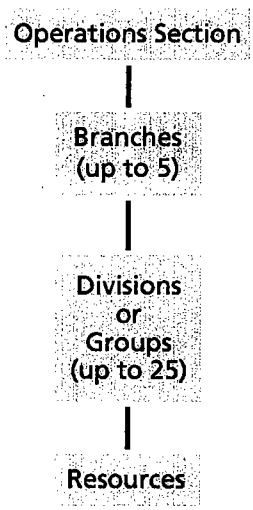

Figure 2-A—Major Organizational Elements of Incident Operations

A. OPERATIONS SECTION CHIEF.

The Operations Section Chief directly manages all incident tactical activities and implements the IAP. The Operations Section Chief may have one or more deputies (preferably from other agencies in multijurisdictional incidents). Deputies will be qualified to a similar level as the Operations Section Chief. An Operations Section Chief should be designated for each operational period and will have direct involvement in the preparation of the IAP for the period of responsibility.

B. DIVISIONS AND GROUPS.

Divisions and groups are established when the number of resources exceeds the Operations Section Chief's manageable span of control. Divisions demarcate physical or geographical areas of operation within the incident area. Groups demarcate functional areas of operation for the incident. See Figure 2-B.

The use of the two terms is necessary, because *division* always refers to a geographical assignment and *group* always refers to a functional assignment. Both divisions and groups may be used in a single incident if there is justification for their use and if proper coordination can be effected.

As additional types of resources are added to the organization, resources should be assigned into a division structure. See Figure 2-C.

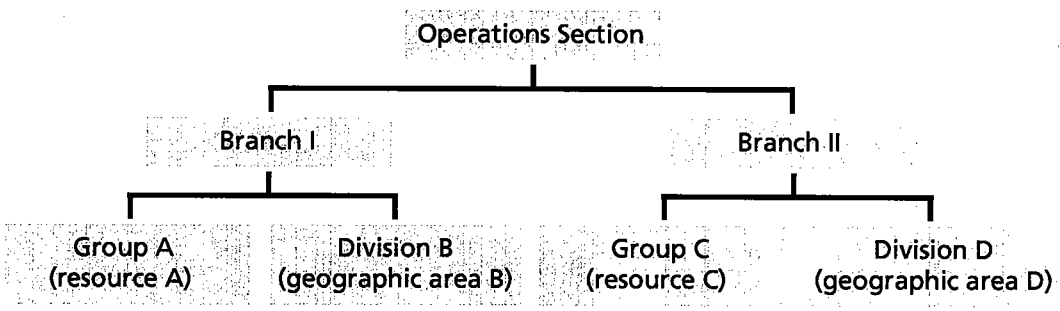

Figure 2-B—Divisions and Groups

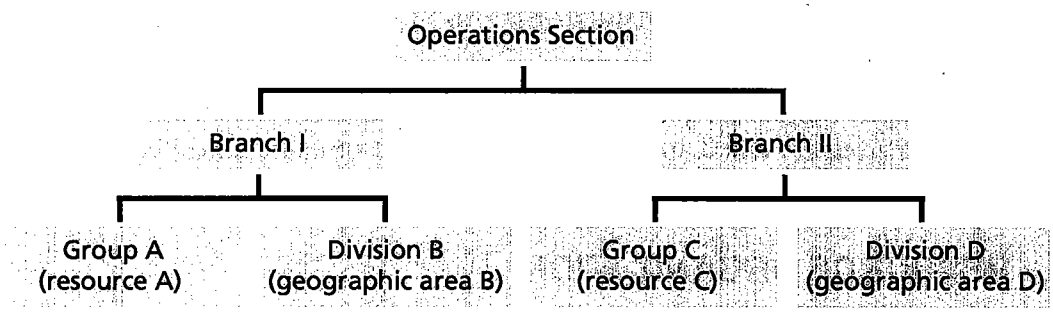

Figure 2-C—Two-Division Organization

1. Geographical Divisions.

The best way to create geographical divisions is to divide an area according to natural separations of terrain or other prominent geographical features, such as rivers. When geographical features are used for determining boundaries, the size of the division should correspond to appropriate span-of-control guidelines. See Figure 2-D.

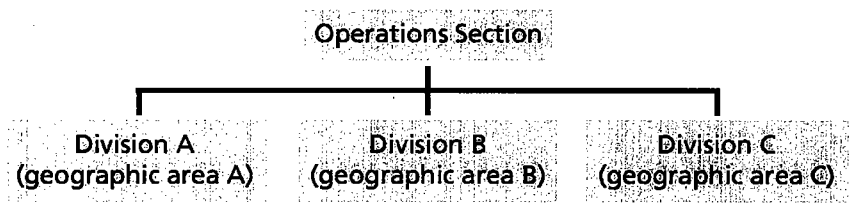

Figure 2-D—Use of Geographical Divisions

2. Functional Groups.

Functional groups can best be used to describe areas of like activity (e.g., rescue, evacuation, medical). See Figure 2-E.

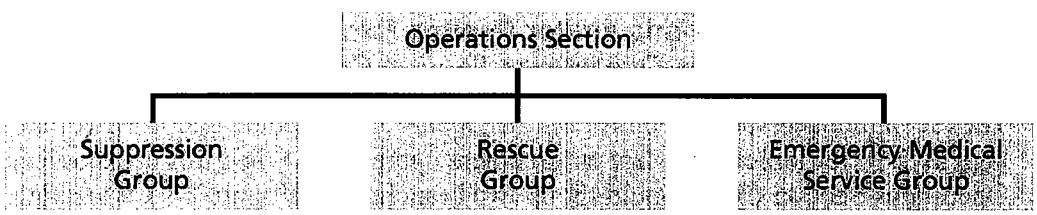

Figure 2-E—Use of Functional Groups

3. Combined Geographical Divisions and Functional Groups.

It is also possible to have both divisions and groups within the Operations Section. For example, Divisions A, B, and C (based on jurisdictional boundaries) might each have two groups, 1 and 2, to provide a management structure for different types of resources within that division.

C. RESOURCE ORGANIZATION.

Initially, in any incident, individual resources that are assigned will report directly to the IC. As the incident grows in size or complexity, individual resources may be organized and employed in a number of ways to facilitate incident management:

1. Single Resources.

Resources may be employed on an individual basis. This is typically the case in the context of the initial response to the incident. During sustained operations, situations will typically arise that call for the use of a single helicopter, vehicle, mobile equipment, etc.

2. Task Forces.

Task Forces are any combination of resources put together to accomplish a specific mission. Task Forces have a designated leader and operate with common communications. Combining resources into Task Forces allows several key resource elements to be managed under one individual's supervision, thus aiding in span of control.

3. Strike Teams.

A Strike Team consists of a set number of resources of the same kind and type operating under a designated leader with common communications between them. Strike Teams represent known capability and are highly effective management units.

D. BRANCHES.

Branches may be established to serve several purposes including the following:

1. The Numbers of Divisions and/or Groups Exceed the Recommended Span of Control for the Operations Section Chief.

The recommended span of control for the Operations Section Chief is 1:5 (or as high as 1:10 for larger-scale law enforcement operations).When this is exceeded, the Operations Section Chief should set up two branches (see Figure 2-F), allocating the divisions and groups between them. For example, if one group and four divisions are reporting to the Operations Section Chief, and two divisions and one group are to be added, a two-branch organization should be formed.

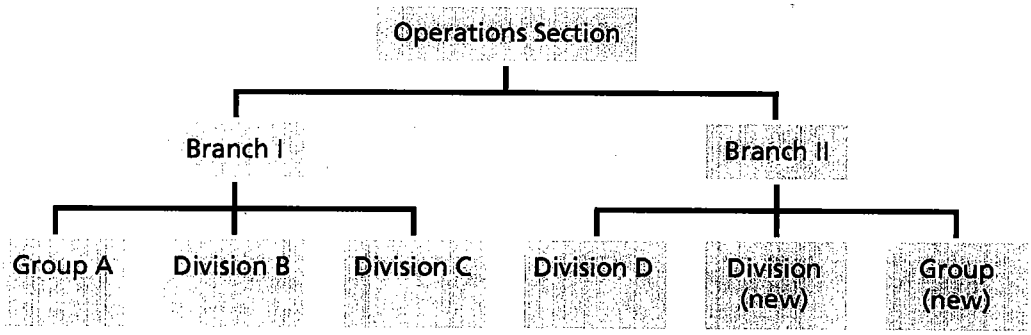

Figure 2-F—Two-Branch Organization

2. The Nature of the Incident Calls for a Functional Branch Structure.

For example, if a large aircraft crashes within a city, various departments within the city (including police, fire, emergency services, and public health services) would each have a functional branch operating under the direction of a single Operations Section Chief. In this example (see Figure 2-G), the Operations Section Chief is from the fire department, with deputies from police and public health services. Other alignments could be made, depending on the city plan and type of emergency. Note that, in this situation, the Incident Command could be either a single command or Unified Command (UC), depending on the jurisdiction.

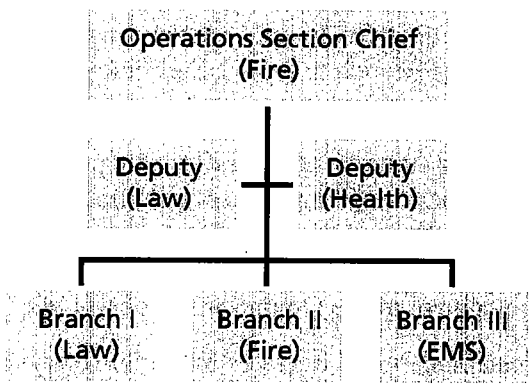

Figure 2-G—Functional Branch Structure

3. The Incident is Multijurisdictional.

In this case, resources are best managed under the agencies that normally control them (see Figure 2-H). For example, the response to a major flood might require combining Federal, State, county, city, and tribal resources.

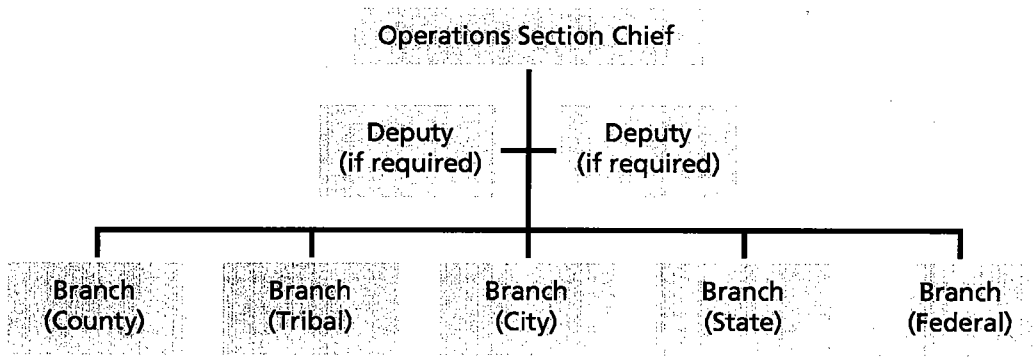

Figure 2-H—Multijurisdictional Incident

E. AIR OPERATIONS BRANCH.

The Operations Section Chief may establish an Air Operations Branch to meet mission requirements in certain situations, in which size, organization, and operation will depend primarily on the nature of the incident and the availability of air assets.[7] Figure 2-I shows a typical organizational structure for air operations.

The Operations Section Chief may designate a director for the Air Operations Branch when the complexity of air operations requires additional support and effort or when the incident requires mixing tactical and logistical utilization of helicopters and other aircraft. Flight safety is a paramount concern in complex operations and supports the requirement for a designated Air Operations Branch to ensure the deconfliction of assets and the integration of safety considerations into operational planning and mission execution.

Whenever both helicopters and fixed-wing aircraft must operate simultaneously within the incident air space, a Air Tactical Group Supervisor should be designated. This individual coordinates all airborne activity with the assistance of a helicopter coordinator and a fixed-wing coordinator. When only one helicopter is used, however, the helicopter may be directly under the control of the Operations Section Chief.

The Air Support Group establishes and operates bases for rotary-wing air assets and maintains required liaison with off-incident fixed-wing bases. The Air Support Group is responsible for all timekeeping for aviation assets assigned to the incident.

[7] Air Operations Branch is used here as an example and may not be applicable to all ICS organizations.

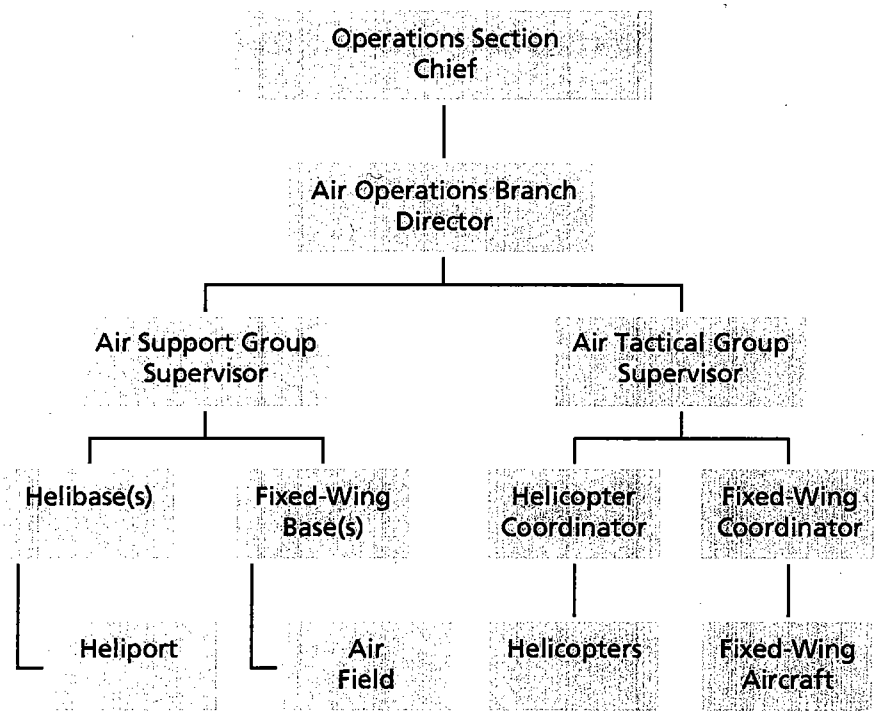

Figure 2-I—Air Operations Organization

(This Page Intentionally Left Blank)

TAB 3—THE PLANNING SECTION

The Planning Section is responsible for collecting, evaluating, and disseminating tactical information pertaining to the incident. This section maintains information and intelligence on the current and forecasted situation, as well as the status of resources assigned to the incident. The Planning Section prepares and documents IAPs and incident maps and gathers and disseminates information and intelligence critical to the incident. As shown in Figure 3-A, the Planning Section has four primary units and may include a number of technical specialists to assist in evaluating the situation and forecasting requirements for additional personnel and equipment.

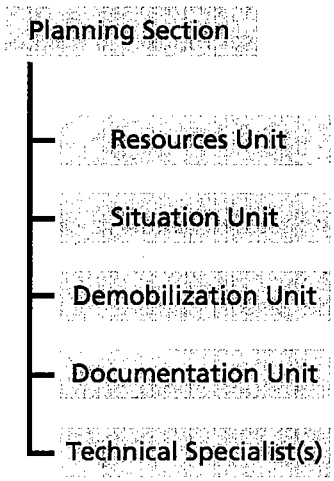

Figure 3-A—Planning Section Organization

A. PLANNING SECTION CHIEF.

The Planning Section Chief oversees all incident-related data gathering and analysis regarding incident operations and assigned resources, develops alternatives for tactical operations, conducts planning meetings, and prepares the IAP for each operational period. This individual will normally come from the jurisdiction with primary incident responsibility and may have one or more deputies from other participating jurisdictions.

B. RESOURCES UNIT.

1. Responsibilities.

Physical resources consist of personnel, teams, facilities, supplies, and major items of equipment available for assignment to or employment during incidents. The Resources Unit makes certain that all assigned personnel and other resources have checked in at the incident. This unit should have a system for keeping track of the current location and status of all assigned resources and should maintain a master list of all resources committed to incident operations.

2. Managing Resources.

For effective management of their employment, resources must be categorized by capability and capacity across disciplines and tracked continuously as to status. The following tools are necessary for maintaining an up-to-date and accurate picture of resource utilization:

a. Status Conditions.

Tactical resources at an incident can have one of three status conditions:

- Assigned resources are personnel, teams, equipment, or facilities that have checked in (or in the case of equipment and facilities, receipted for) and are supporting incident operations.
- Available resources are personnel, teams, equipment, or facilities that have been assigned to an incident and are ready for a specific work detail or function.
- Out-of-service resources are personnel, teams, equipment, or facilities that have been assigned to an incident but are unable to function for mechanical, rest, or personal reasons; or because their condition makes them unusable.

b. Changes in Status.

Normally, the individual who changes the status of a resource, such as equipment location and status, is responsible for promptly informing the Resources Unit.

C. SITUATION UNIT.

The Situation Unit collects, processes, and organizes ongoing situation information; prepares situation summaries; and develops projections and forecasts of future events related to the incident. The Situation Unit also prepares maps and gathers and disseminates information and intelligence for use in the IAP. This unit may also require the expertise of technical specialists and operations and information security specialists.

D. DOCUMENTATION UNIT.

The Documentation Unit maintains accurate and complete incident files, including a complete record of the major steps taken to resolve the incident; provides duplication services to incident personnel; and files, maintains, and stores incident files for legal, analytical, and historical purposes. Documentation is part of the Planning Section primarily because this unit prepares the IAP and maintains many of the files and records that are developed as part of the overall IAP and planning function.

E. DEMOBILIZATION UNIT.

The Demobilization Unit develops an Incident Demobilization Plan that includes specific instructions for all personnel and resources that will require demobilization. This unit should begin its work early in the incident, creating rosters of personnel and resources and obtaining any missing information as check-in proceeds.

Note that many city- and county-provided resources, because they are local, do not require specific demobilization instructions. Once the Incident Demobilization Plan has been approved, the Demobilization Unit ensures that it is distributed both at the incident and elsewhere as necessary.

F. TECHNICAL SPECIALISTS.

The ICS is designed to function in a wide variety of incident scenarios requiring the use of technical specialists. These personnel have special skills and are activated only when needed. Specialists may serve anywhere within the organization, including the Command Staff. No minimum qualifications are prescribed, as technical specialists normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically specially certified in their fields or professions.

Technical specialists assigned to the Planning Section may report directly to its chief, may report to any function in an existing unit, or may form a separate unit within the Planning Section, depending on the requirements of the incident and the needs of the Section Chief. Technical specialists may also be assigned to other parts of the organization (e.g., to the Operations Section to assist with tactical matters or to the Finance/Administration Section to assist with fiscal matters). For example, a legal specialist or 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. Generally, if the expertise is needed for only a short period and normally involves only one individual, that individual should be assigned to the Situation Unit. If the expertise will be required on a long-term basis and may require several personnel, it is advisable to establish a separate Technical Unit in the Planning Section.

The incident itself will primarily dictate the needs for technical specialists. Below are representative examples of the kinds of specialists that may be required:

- meteorologist
- environmental impact specialist
- resource use and cost specialists
- flood control specialist
- water-use specialist
- explosives specialist
- structural engineering specialist
- firefighter specialist
- medical and/or health care specialist
- medical intelligence specialist
- pharmaceutical specialist
- veterinarian
- agricultural specialist
- toxic substance specialist
- radiation health physicist
- intelligence specialist
- infectious disease specialist
- chemical or radiological decontamination specialist
- law enforcement specialist
- attorney or legal counsel
- industrial hygienist
- transportation specialist
- scientific support coordinator.

A specific example of the need to establish a distinct technical unit within the General Staff is the requirement to coordinate and manage large volumes of environmental sampling and/or analytical data from multiple sources in the context of certain complex incidents, particularly those involving biological, chemical, and radiation hazards. To meet this requirement, an Environmental Unit could be established within the Planning Section to facilitate interagency environmental data management, monitoring, sampling, analysis, and assessment. The Environmental Unit would prepare environmental data for the Situation Unit and work in close coordination with other units and sections within the ICS structure to enable effective decision support to the IC or UC. Technical Specialists assigned to the Environmental Unit might include a Scientific Support Coordinator and Sampling, Response Technologies, Weather Forecast, Resources at Risk, Cleanup

Assessment, and Disposal Technical Specialists. Example tasks accomplished by the Environmental Unit would include the following:

- identifying sensitive areas and recommending response priorities;
- developing a plan for collecting, transporting, and analyzing samples;
- providing input on wildlife protection strategies;
- determining the extent and effects of site contamination;
- developing site cleanup and hazardous material disposal plans; and
- identifying the need for and obtaining permits and other authorizations.

(This Page Intentionally Left Blank)

TAB 4—THE LOGISTICS SECTION

The Logistics Section meets all support needs for the incident, including ordering resources through appropriate procurement authorities from off-incident locations. It also provides facilities, transportation, supplies, equipment maintenance and fueling, food service, communications, and medical services for incident personnel. See Figure 4-A.

The Logistics Section is led by a Section Chief, who may also have a deputy. Having a deputy is encouraged when all designated units are established at an incident site. When the incident is very large or requires a number of facilities with large numbers of equipment, the Logistics Section can be divided into two branches (Figure 4-B provides an example).

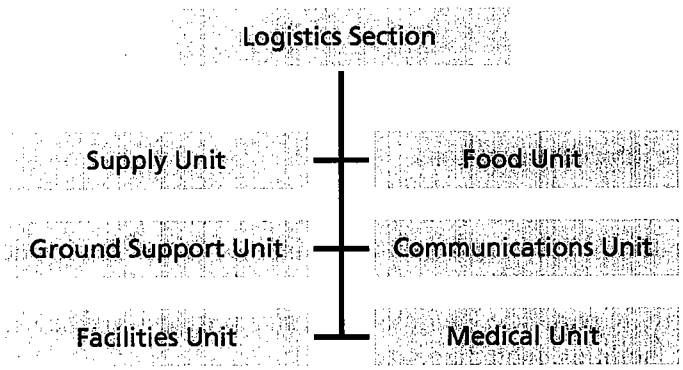

Figure 4-A—Logistics Section Organization

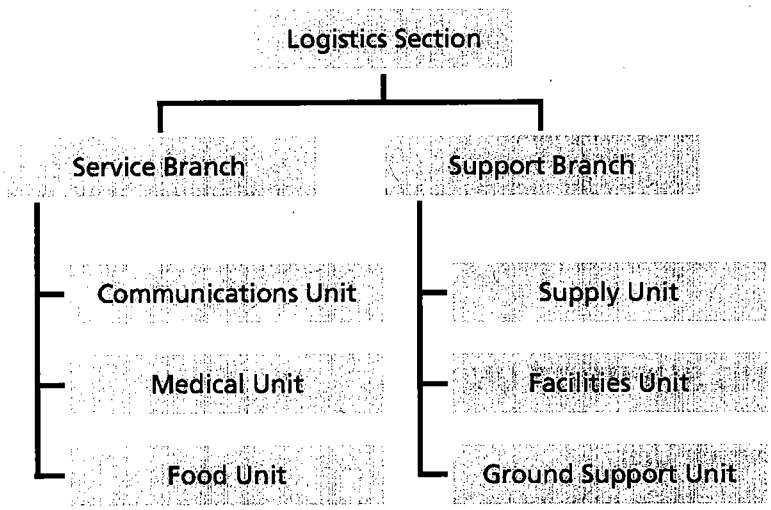

Figure 4-B—Logistics Section: Two-Branch Organizational Structure

A. SUPPLY UNIT.

The Supply Unit orders, receives, stores, and processes all incident-related resources, personnel, and supplies.

Once established, the Supply Unit also has the basic responsibility for all off-incident ordering, including

- all tactical and support resources (including personnel)
- all expendable and nonexpendable supplies required for incident support.

The Supply Unit provides the support required to receive, process, store, and distribute all supply orders. The unit also handles tool operations, which include storing, disbursing, and servicing of all tools and portable, nonexpendable equipment.

B. FACILITIES UNIT.

The Facilities Unit sets up, maintains, and demobilizes all facilities used in support of incident operations. The unit also provides facility maintenance and security services required to support incident operations.

The Facilities Unit sets up the ICP, incident base, and camps, as well as trailers and/or other forms of shelter for use in and around the incident area. The incident base and camps may often be established in areas having existing structures, which may be used in their entirety or only in part. The Facilities Unit also provides and sets up necessary personnel support facilities, including areas for

- food and water service;
- sleeping;
- sanitation and showers; and
- staging.

This unit also orders, through supply, such additional support items as portable toilets, shower facilities, and lighting units.

Note that providing shelter for victims is a critical operational activity, which will be incorporated into the IAP. Sheltering will normally be conducted by appropriate nongovernmental organization staff, such as the American Red Cross or other similar entities.

C. GROUND SUPPORT UNIT.

The Ground Support Unit

- maintains and repairs primary tactical equipment, vehicles, and mobile ground support equipment;

- records usage time for all ground equipment (including contract equipment) assigned to the incident;
- supplies fuel for all mobile equipment;
- provides transportation in support of incident operations (except aircraft); and
- develops and implements the Incident Traffic Plan.

In addition to its primary functions of maintaining and servicing vehicles and mobile equipment, the Ground Support Unit also maintains a transportation pool for major incidents. This pool consists of vehicles (e.g., staff cars, buses, pick-ups) that are suitable for transporting personnel. The Ground Support Unit also provides up-to-date information on the location and status of transportation vehicles to the Resources Unit.

D. COMMUNICATIONS UNIT.

The Communications Unit develops the Communications Plan (ICS205) to make the most effective use of the communications equipment and facilities assigned to the incident, installs and tests all communications equipment, supervises and operates the incident communications center, distributes and recovers communications equipment assigned to incident personnel, and maintains and repairs communications equipment on site.

The Communications Unit's major responsibility is effective communications planning for the ICS, especially in the context of a multiagency incident. This is critical for determining required radio nets, establishing interagency frequency assignments, and ensuring the interoperability and the optimal use of all assigned communications capabilities.

The Communications Unit Leader should attend all incident-planning meetings to ensure that the communication systems available for the incident can support tactical operations planned for the next operational period.

Incident communications are managed through the use of a common communications plan and an incident-based communications center established solely for the use of tactical and support resources assigned to the incident.

Advance planning is required to ensure that an appropriate communications system is available to support incident operations requirements. This planning includes the development of frequency inventories, frequency-use agreements, and interagency radio caches.

Most complex incidents will require an Incident Communications Plan. The Communications Unit is responsible for planning the use of radio frequencies; establishing networks for command, tactical, support, and air units; setting up on-site telephone and public address equipment; and providing any required off-incident communication links. Codes should not be used for radio communication; a clear spoken message—based on common terminology that avoids misunderstanding in complex and noisy situations—reduces the chances for error.

Radio networks for large incidents will normally be organized as follows:

1. Command Net.

Links together: incident command, command staff, section chiefs, branch directors, division, and group supervisors.

2. Tactical Nets.

Several tactical nets may be established to connect agencies, departments, geographical areas, or specific functional units. The determination of how nets are set up should be a joint planning, operations, and logistics function. The Communications Unit Leader will develop the overall plan.

3. Support Net.

A support net may be established primarily to handle changes in resource status but also to handle logistical requests and other nontactical functions.

4. Ground-to-Air Net.

To coordinate ground-to-air traffic, either a specific tactical frequency may be designated, or regular tactical nets may be used.

5. Air-to-Air Nets.

Air-to-air nets will normally be predesignated and assigned for use at the incident.

E. FOOD UNIT.

The Food Unit determines food and water requirements; plans menus, orders food, provides cooking facilities, cooks, serves, maintains food service areas, and manages food security and safety concerns.

Efficient food service is important, but especially so for any extended incident. The Food Unit must be able to anticipate incident needs, both in terms of the number of people who will need to be fed and whether the type, location, or complexity of the incident indicates that there may be special food requirements. The unit must supply food needs for the entire incident, including all remote locations (i.e., camps and staging areas), as well as supply food service to operations personnel unable leave operational assignments. The Food Unit must interact closely with the following elements:

- Planning Section, to determine the number personnel that must be fed;
- Facilities Unit, to arrange food-service areas;
- Supply Unit, to order food;

- Ground Support Unit, to obtain ground transportation; and
- Air Operations Branch Director, to obtain air transportation.

Careful planning and monitoring is required to ensure food safety before and during food service operations, including the assignment, as indicated, of public health professionals with expertise in environmental health and food safety.

Note that feeding victims is a critical operational activity, which will be incorporated into the IAP. Feeding activities will normally be conducted by members of an appropriate nongovernmental organization, such as the American Red Cross or similar entities.

F. MEDICAL UNIT.

The primary responsibilities of the Medical Unit include the following:

- develop the Incident Medical Plan (for incident personnel);
- develop procedures for handling any major medical emergency involving incident personnel;
- provide continuity of medical care, including vaccinations, vector control, occupational health, prophylaxis, and mental health services for incident personnel;
- provide transportation for injured incident personnel;
- ensure that incident personnel patients are tracked as they move from origin, to care facility, to final disposition;
- assist in processing all paperwork related to injuries or deaths of incident assigned personnel; and
- coordinate personnel and mortuary affairs for incident personnel fatalities.

The Medical Unit is responsible for the effective and efficient provision of medical services to incident personnel. The Medical Unit Leader will develop a medical plan, which will, in turn, form part of the IAP. The medical plan should provide specific information on medical assistance capabilities at incident locations, potential hazardous areas or conditions, and off-incident medical assistance facilities and procedures for handling complex medical emergencies. The Medical Unit will also assist the Finance/Administration Section with the administrative requirements related to injury compensation, including obtaining written authorizations, billing forms, witness statements, administrative medical documents, and reimbursement as required. The Medical Unit will ensure patient privacy to the fullest extent possible.

Note that patient care and medical services for those who are not incident personnel (victims of a bioterror attack, hurricane victims, etc.) are critical operational activities associated with a host of potential incident scenarios. As such, these activities are incorporated into the IAP as key considerations of the Plans and Operations Sections. These sections should be staffed accordingly with appropriately qualified Emergency Medical Services public health, medical personnel, technical experts, and other professional personnel, as required.

(This Page Intentionally Left Blank)

TAB 5—THE FINANCE/ADMINISTRATION SECTION

When there is a specific need for financial, reimbursement (individual and agency or department), and/or administrative services to support incident management activities, a Finance/Administration Section is established. Under the ICS, not all agencies will require such assistance. In large, complex scenarios involving significant funding originating from multiple sources, the Finance/Administrative Section is an essential part of the ICS. In addition to monitoring multiple sources of funds, the Section Chief must track and report to the IC the financial "burn rate" as the incident progresses. This allows the IC to forecast the need for additional funds before operations are affected negatively. This is particularly important if significant operational assets are under contract from the private sector. The Section Chief may also need to monitor cost expenditures to ensure that statutory rules that apply are met. Close coordination with the Planning Section and Logistics Section is also essential so that operational records can be reconciled with financial documents. Note that, in some cases, only one specific function may be required (e.g., cost analysis), which a technical specialist in the Planning Section could provide. Figure 5-A illustrates the basic Finance/Administration Section organizational structure.

The Finance/Administration Section Chief will determine, given current and anticipated future requirements, the need for establishing specific subordinate units. In some of the functional areas (e.g., procurement), an actual unit need not be established if it would consist of only one person. In such a case, a procurement technical specialist would be assigned in the Planning Section instead. Because of the specialized nature of finance functions, the Section Chief should come from the agency that has the greatest requirement for this support. The Section Chief may have a deputy

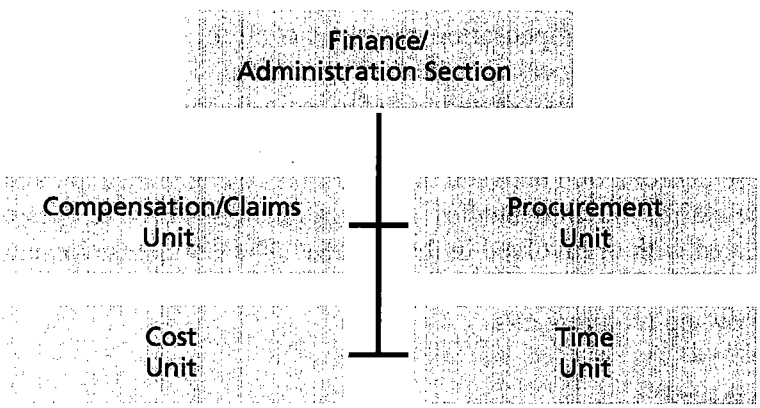

Figure 5-A—Finance and Administration Section Organization

A. TIME UNIT.

The Time Unit is primarily responsible for ensuring proper daily recording of personnel time, in accordance with the policies of the relevant agencies. The Time Unit also ensures that the Logistics Section records or captures equipment usage time, through the Ground Support Unit for ground equipment and through the Air Operations Support Group for aircraft.

If applicable (depending on the agencies involved), personnel time records will be collected and processed for each operational period. The unit leader may require the assistance of personnel familiar with the relevant policies of any affected agencies. These records must be verified, checked for accuracy, and posted according to existing policies. Excess hours worked must also be determined, for which separate logs must be maintained.

B. PROCUREMENT UNIT.

The Procurement Unit administers all financial matters pertaining to vendor contracts. This unit coordinates with local jurisdictions to identify sources for equipment, prepares and signs equipment rental agreements, and processes all administrative requirements associated with equipment rental and supply contracts.

Note that, in some agencies, the Supply Unit in the Logistics Section will be responsible for certain procurement activities. The Procurement Unit will also work closely with local cost authorities.

C. COMPENSATION AND CLAIMS UNIT.

Under ICS, a single unit handles injury compensation and claims. The specific activities are, of course, varied and may not always be accomplished by the same person. The individual handling injury compensation ensures that all forms required by workers' compensation programs and local agencies are completed. This individual also maintains files on injuries and illnesses associated with the incident and ensures that all witness statements are obtained in writing. Since the Medical Unit may also perform certain of these tasks, close coordination between the Medical and Compensation and Claims Units is essential. The claims function handles investigations of all civil tort claims involving property associated with or involved in the incident. The Compensation and Claims Unit maintains logs on the claims, obtains witness statements, and documents investigations and agency follow-up requirements.

D. COST UNIT.

The Cost Unit provides cost analysis data for the incident. This unit must ensure that equipment and personnel for which payment is required are properly identified, obtain

and record all cost data, and analyze and prepare estimates of incident costs. The Cost Unit also provides input on cost estimates for resource use to the Planning Section. The Cost Unit must maintain accurate information on the actual costs of all assigned resources.

(This Page Intentionally Left Blank)

TAB 6—ESTABLISHING AN AREA COMMAND

An Area Command is established when the complexity of the incident and incident management span-of-control considerations so dictate. Generally, the administrator(s) of the agency having jurisdictional responsibility for the incident makes the decision to establish an Area Command.

The purpose of an Area Command is 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 or complex incident that has multiple incident management teams engaged.

This type of command is generally used when there are a number of incidents in the same area and of the same type, such as two or more HAZMAT spills or fires. These are usually the kinds of incidents that may compete for the same resources. When incidents are of different types and/or do not have similar resource demands, they are usually handled as separate incidents or are coordinated through an EOC. If the incidents under the authority of the Area Command span multiple jurisdictions, a Unified Area Command should be established. This allows each jurisdiction involved to have appropriate representation in the Area Command.

Area Commands are particularly relevant to public health emergencies, given that these events are typically not site specific, not immediately identifiable, geographically dispersed, and evolve over time ranging from days to weeks. Such events as these, as well as acts of biological, chemical, radiological, and nuclear terrorism, call for a coordinated intergovernmental, private-sector, and nongovernmental organization response, with large-scale coordination typically conducted at a higher jurisdictional level.

A. RESPONSIBILITIES.

The Area Command does not have operational responsibilities. For the incidents under its authority, the Area Command:

- sets overall agency incident-related priorities;
- allocates critical resources according to the established priorities;
- ensures that incidents are properly managed;
- ensures effective communications;
- ensures that incident management objectives are met and do not conflict with each other or with agency policies;
- identifies critical resource needs and reports them to the interagency coordination system (generally EOCs);

- ensures that short-term "emergency" recovery is coordinated to assist in the transition to full recovery operations; and
- provides for personnel accountability and a safe operating environment.

The Area Command develops an action plan detailing incident management priorities, needs, and objectives. This plan should clearly state policy, objectives, and priorities; provide a structural organization with clear lines of authority and communications; and identify incident management functions to be performed by the Area Command (i.e., public communications).

B. ORGANIZATION.

The Area Command organization operates under the same basic principles as ICS. Typically, an Area Command will comprise the following key personnel, all of whom must possess appropriate qualifications and certifications:

1. Area Commander (Unified Area Command).

The Area Commander is responsible for the overall direction of the incident management teams assigned to the same incident or to incidents in close proximity. This responsibility includes ensuring that conflicts are resolved, that incident objectives are established, and that strategies are selected for the use of critical resources. The Area Command is also responsible for coordinating with Federal, State, local, tribal, and participating private organizations.

2. Area Command Logistics Chief.

The Area Command Logistics Chief provides facilities, services, and materials at the Area Command level and ensures the effective allocation of critical resources and supplies among the incident management teams.

3. Area Command Planning Chief.

The Area Command Planning Chief collects information from various incident management teams to assess and evaluate potential conflicts in establishing incident objectives, strategies, and priorities for allocating critical resources.

4. Area Command Support Positions.

The following positions are activated as necessary.

a. Area Command Critical Resources Unit Leader.

The critical resources unit leader tracks and maintains the status and availability of critical resources assigned to each incident under the Area Command.

b. *Area Command Situation Unit Leader.*

The situation unit leader monitors the status of objectives for each incident or IMT assigned to the area command.

c. *Area Command Public Information Officer.*

The PIO provides public information coordination between incident locations and serves as the point of contact for media requests to the Area Command.

d. *Area Command Liaison Officer.*

The liaison officer helps maintain off-incident interagency contacts and coordination.

e. *Area Command Aviation Coordinator.*

An aviation coordinator is assigned when aviation resources are competing for common airspace and critical resources, and works in coordination with incident aviation organizations to evaluate potential conflicts, develop common airspace management procedures, and prioritize critical resources.

C. LOCATION.

The following guidelines should be followed in locating an Area Command:

- To the extent possible, the area command should be established in close proximity to the incidents under its authority. This makes it easier for the Area Commander and the ICs to meet and otherwise interact.
- It is, however, best not to collocate an Area Command with any individual ICP. Doing so might cause confusion with the command and management activities associated with that particular incident.
- Area commands must establish effective, efficient communications and coordination processes and protocols with subordinate ICPs, as well as with other incident management organizations involved in incident operations.
- The facility used to house the organization should be large enough to accommodate a full Area Command staff. It should also be able to accommodate meetings between the Area Command staff, the ICs, and agency executive(s), as well as news media representatives.
- Area Commands may be collocated with EOCs.

D. REPORTING RELATIONSHIPS.

When an Area Command is involved in coordinating multiple incident management activities, the following reporting relationships will apply:

- The ICs for the incidents under the Area Command's authority report to the Area Commander.
- The Area Commander is accountable to the agency(s) or to the jurisdictional executive(s) or administrator(s).
- If one or more incidents within the Area Command are multijurisdictional, a Unified Area Command should be established. In this instance, ICs would report to the Unified Area Commander for their jurisdiction.

TAB 7—PREDESIGNATED FACILITIES AND AREAS

Several kinds and types of facilities may be established in and around the incident area. The requirements of the incident and the desires of the IC will determine the specific kinds of facilities used and their locations and may consist of the following designated facilities, among various others:

A. INCIDENT COMMAND POST.

The ICP signifies the location of the tactical-level, on-scene incident command and management organization. It typically comprises the IC and immediate staff and may include other designated incident management officials and responders from Federal, State, local, and tribal agencies, as well as private-sector and nongovernmental organizations. Typically, the ICP is located at or in the immediate vicinity of the incident site and is the locus for the conduct of direct, on-scene control of tactical operations. Incident planning is also conducted at the ICP; an incident communications center also would normally be established at this location. The ICP may be collocated with the incident base, if the communications requirements can be met. The ICP may perform local EOC-like functions in the context of smaller jurisdictions or less complex incident scenarios.

B. INCIDENT BASE.

An Incident Base is the location at which primary support activities are conducted. A single incident base is established to house all equipment and personnel support operations. The Logistics Section, which orders all resources and supplies, is also located at this base. The Incident Base should be designed to be able to support operations at multiple incident sites.

C. CAMPS.

Camps are separate from the Incident Base and are located in satellite fashion from the Incident Base where they can best support incident operations. Camps provide certain essential auxiliary forms of support, such as food, sleeping areas, and sanitation. Camps may also provide minor maintenance and servicing of equipment. Camps may be relocated to meet changing operational requirements.

D. MOBILIZATION AND STAGING AREAS.

Staging areas are established for temporary location of available resources. Staging Areas will be established by the Operations Section Chief to enable positioning of and

accounting for resources not immediately assigned. A Staging Area can be any location in which personnel, supplies, and equipment can be temporarily housed or parked while awaiting operational assignment. Staging Areas may include temporary feeding, fueling, and sanitation services. The Operations Section Chief assigns a manager for each Staging Area, who checks in all incoming resources, dispatches resources at the Operations Section Chief's request, and requests Logistics Section Support, as necessary, for resources located in the Staging Area. Personnel check in with the Resources Unit at the Staging Area, while supplies and equipment are checked in with the Supply Unit. If neither of these functions is activated, resources report to the Staging Area Manager for direction.

TAB 8—THE PLANNING PROCESS

A. OVERVIEW.

Sound, timely planning provides the foundation for effective domestic incident management. The NIMS planning process described below represents a template for strategic, operational, and tactical planning that includes all steps an IC and other members of the Command and General Staffs should take to develop and disseminate an Incident Action Plan (IAP). The planning process may begin with the scheduling of a planned event, the identification of a credible threat, or with the initial response to an actual or impending event. The process continues with the implementation of the formalized steps and staffing required to develop a written IAP.

A clear, concise IAP template is essential to guide the initial incident management decision process and the continuing collective planning activities of incident management teams. The planning process should provide the following:

- current information that accurately describes the incident situation and resource status;
- predictions of the probable course of events;
- alternative strategies to attain critical incident objectives; and
- an accurate, realistic, IAP for the next operational period.

Five primary phases must be followed, in sequence, to ensure a comprehensive IAP. These phases are designed to enable the accomplishment of incident objectives within a specified time. The IAP must provide clear strategic direction and include a comprehensive listing of the tactical objectives, resources, reserves, and support required to accomplish each overarching incident objective. The comprehensive IAP will state the sequence of events in a coordinated way for achieving multiple incident objectives.

The primary phases of the planning process are essentially the same for the IC who develops the initial plan, for the IC and Operations Section Chief revising the initial plan for extended operations, and for the incident management team developing a formal IAP, each following a similar process. During the initial stages of incident management, planners must develop a simple plan that can be communicated through concise oral briefings. Frequently, this plan must be developed very quickly and with incomplete situation information. As the incident management effort evolves over time, additional lead-time, staff, information systems, and technologies enable more detailed planning and cataloging of events and "lessons learned."

The five primary phases in the planning process are:

1. Understand the Situation.

The first phase includes gathering, recording, analyzing, and displaying situation and resource information in a manner that will ensure

- a clear picture of the magnitude, complexity, and potential impact of the incident; and
- the ability to determine the resources required to develop and implement an effective IAP.

2. Establish Incident Objectives and Strategy.

The second phase includes formulating and prioritizing incident objectives and identifying an appropriate strategy. The incident objectives and strategy must conform to the legal obligations and management objectives of all affected agencies.

Reasonable alternative strategies that will accomplish overall incident objectives are identified, analyzed, and evaluated to determine the most appropriate strategy for the situation at hand. Evaluation criteria include public health and safety factors; estimated costs; and various environmental, legal, and political considerations.

3. Develop the Plan.

The third phase involves determining the tactical direction and the specific resource, reserves, and support requirements for implementing the selected strategy for one operational period. This phase is usually the responsibility of the IC, who bases decisions on resources allocated to enable a sustained response. After determining the availability of resources, the IC develops a plan that makes the best use of these resources.

Prior to the formal planning meetings, each member of the Command Staff and each functional Section Chief is responsible for gathering certain information to support these decisions. During the Planning Meeting, the Section Chiefs develop the plan collectively.

4. Prepare and Disseminate the Plan.

The fourth phase involves preparing the plan in a format that is appropriate for the level of complexity of the incident.

For the initial response, the format is a well-prepared outline for an oral briefing. For most incidents that will span multiple operational periods, the plan will be developed in writing according to ICS procedures.

5. Evaluate and Revise the Plan.

The planning process includes the requirement to evaluate planned events and check the accuracy of information to be used in planning for subsequent operational periods. The General Staff should regularly compare planned progress with actual

progress. When deviations occur and when new information emerges, that information should be included in the first step of the process used for modifying the current plan or developing the plan for the subsequent operational period.

B. RESPONSIBILITIES AND SPECIFIC PLANNING ACTIVITIES.

The following is a checklist of planning responsibilities and specific planning activities:

1. General Responsibilities.

The general responsibilities associated with the Planning Meeting and the development of the IAP are described below. The Planning Section Chief should review these with the General Staff prior to the planning meeting.

a. Planning Section Chief.

- Conduct the Planning Meeting and coordinate preparation of the IAP.

b. Incident Commander.

- Provide overall control objectives and strategy.
- Establish procedures for off-incident resource ordering.
- Establish procedures for resource activation, mobilization, and employment.
- Approve completed IAP plan by signature.

c. Finance Section Chief.

- Provide cost implications of control objectives, as required.
- Evaluate facilities being used to determine if any special arrangements are needed.
- Ensure that the IAP is within the financial limits established by the IC.

d. Operations Section Chief.

- Determine division work assignments and resource requirements.

e. Logistics Section Chief.

- Ensure that incident facilities are adequate.
- Ensure that the resource ordering procedure is made known to appropriate agency dispatch center(s).
- Develop a transportation system to support operational needs.
- Ensure that the section can logistically support the IAP.
- Place order(s) for resources.

2. Preplanning Steps: Understanding the Problem and Establishing Objectives and Strategy.

The Planning Section Chief should take the following actions prior to the initial Planning Meeting (if possible, obtaining a completed Incident Briefing Form ICS 201):

- Evaluate the current situation and decide whether the current planning is adequate for the remainder of the operational period (i.e., until next plan takes effect).
- Advise the IC and the Operations Section Chief of any suggested revisions to the current plan, as necessary.
- Establish a planning cycle for the IC.
- Determine Planning Meeting attendees in consultation with the IC. For major incidents, attendees should include
  - Incident Commander
  - Command Staff members
  - General Staff members
  - Resources Unit Leader
  - Situation Unit Leader
  - Air Operations Branch Director (if established)
  - Communications Unit Leader
  - Technical and/or Specialists (as required)
  - Agency representatives (as required).
- Establish the location and time for the Planning Meeting.
- Ensure that planning boards and forms are available.
- Notify necessary support staff about the meeting and their assignments.
- Ensure that a current situation and resource briefing will be available for the meeting.
- Obtain an estimate of regional resource availability from agency dispatch for use in planning for the next operational period.
- Obtain necessary agency policy, legal, or fiscal constraints for use in the Planning Meeting.

3. Conducting the Planning Meeting.

The Planning Meeting is normally conducted by the Planning Section Chief. The checklist that follows is intended to provide a basic sequence of steps to aid the Planning Section Chief in developing the IAP. The planning checklist is used with

the ICS Planning Matrix Board and/or ICS Form 215—*Operational Planning Worksheet.*[8] (The worksheet is laid out in the same manner as the Planning Matrix Board.) Every incident must have an action plan. However, not all incidents require written plans. The need for written plans and attachments is based on the requirements of the incident and the decision of the IC.

The Planning Meeting checklist is as follows:

- give briefing on situation and resource status (Planning Section)
- set control objectives (IC)
- plot control lines and division boundaries (Operations Section)
- specify tactics for each Division or Group (Operations Section)
- specify resources needed by Division or Group (Operations Section, Planning Section)
- specify facilities and reporting locations plot on map (Operations Section, Planning Section, Logistics Section)
- place resource and overhead personnel order (Logistics Section)
- consider communications, medical, and traffic plan requirements (Planning Section, Logistics Section)
- finalize, approve, and implement IAP (IC, Planning Section, Operations Section).

4. Brief on Situation and Resource Status.

The Planning Section Chief and/or Resources and Situation Unit Leaders should provide an up-to-date briefing on the situation. Information for this briefing may come from any or all of the following sources:

- Initial Incident Commander
- Incident Briefing Form (ICS 201)
- field observations
- operations reports
- regional resources and situation reports.

5. Set Control Objectives.

This step is accomplished by the IC. The control objectives are not limited to any single operational period but will consider the total incident situation. The IC will establish the general strategy to be used; will state any major policy, legal, or fiscal

[8] For examples of ICS Forms, see Appendix A, Tab 9.

constraints on accomplishing the objectives; and will offer appropriate contingency considerations.

6. Plot Control Lines and Division Boundaries on Map.

This step is normally accomplished by the Operations Section Chief (for the next operational period) in conjunction with the Planning Section Chief who will determine control line locations, establish division and branch boundaries for geographical divisions, and determine the need for functional group assignments for the next operational period. These will be plotted on the map.

7. Specify Tactics for Each Division.

After determining division geographical assignments, the Operations Section Chief will establish the specific work assignments to be used for each division for the next operational period. (Note that it may be necessary or desirable to establish a functional group in addition to geographical divisions.) Tactics (work assignments) must be specific and must be within the boundaries set by the IC's general control objectives (strategies). These work assignments should be recorded on the planning matrix. The IC, Operations Section Chief, and Logistics Section Chief should also at this time consider the need for any alternative strategies or tactics and ensure that these are properly noted on the planning matrix.

8. Specify Resources Needed by Division.

After specifying tactics for each division, the Operations Section Chief, in conjunction with the Planning Section Chief, will determine the resource needs by division to accomplish the work assignments. Resource needs will be recorded on the planning matrix. Resource needs should be considered on basis of the type of resources required to accomplish the assignment.

9. Specify Operations Facilities and Reporting Locations and Plot on Map.

The Operations Section Chief, in conjunction with the Planning and Logistics Section Chiefs, should designate and make available the facilities and reporting locations required to accomplish Operations Section work assignments. The Operations Section Chief should also at this time indicate the reporting time requirements for the resources and any special resource assignments.

10. Place Resource and Personnel Order.

At this time, the Planning Section Chief should assess resource needs assessment using the needs indicated by the Operations Section Chief and resources data available from the Planning Section's Resources Unit. The planning matrix, when

properly completed, will show resource requirements and the resources available to meet those requirements. Subtracting the resources available from those required will indicate any additional resource needs. From this assessment, a new resource order can be developed and provided to the IC for approval and then placed through normal dispatch channels by the Logistics Section.

11. Consider Communications, Medical, and Traffic Plan Requirements.

The IAP will normally consist of the Incident Objectives (ICS 202), Organization Chart (ICS 203), Division Assignment List (ICS 204), and a map of the incident area. Larger incidents may require additional supporting attachments, such as a separate Communications Plan (ICS 205), a Medical Plan (ICS 206), and possibly a Traffic Plan. (For examples of ICS forms, see Appendix A, Tab 9.) The Planning Section Chief must determine the need for these attachments and ensure that the appropriate units prepare such attachments. For major incidents, the IAP and attachments will normally include the items listed in Table A-2.

Components	Normally Prepared By
Common Components	
Incident Objectives (ICS 202)	Incident Commander
Organization List or Chart (ICS 203)	Resources Unit
Assignment List (ICS 204)	Resources Unit
Communications Plan (ICS 205)	Communications Unit
Logistics Plan	Logistics Unit
Responder Medical Plan (ICS 206)	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

Table A-2—The IAP and Typical Attachments

Prior to the completion of the plan, the Planning Section Chief should review the division and group tactical work assignments for any changes due to lack of resource availability.

The Resource Unit may then transfer division assignment information including alternatives from the planning matrix board or form (ICS 215) onto the Division Assignment Lists (ICS 204).

12. Finalize, Approve, and Implement the Incident Action Plan.

The Planning Section is responsible for seeing that the IAP is completed, reviewed, and distributed. The following is the sequence of steps for accomplishing this:

- Set the deadline for completing IAP attachments.
- Obtain plan attachments and review them for completeness and approvals.
- Determine the number of IAPs required.
- Arrange with the Documentation Unit to reproduce the IAP.
- Review the IAP to ensure it is up to date and complete prior to the operations briefing and plan distribution.
- Provide the IAP briefing plan, as required, and distribute the plan prior to beginning of the new operational period.

Number	Purpose
ICS-201 (p.1)	Incident Briefing
ICS-201 (p.2)	Summary of Current Actions
ICS-201 (p.3)	Current Organization
ICS-201 (p.4)	Resources Summary
ICS-202	Incident Objectives
ICS-203	Organization Assignment List
ICS-204	Assignment List
ICS-205	Incident Radio Communications Plan
ICS-206	Medical Plan
ICS-207	Organizational Chart
ICS-209	Incident Status Summary, with Instructions
ICS-210	Status Change Card
ICS-211	Check-In-List
ICS-213	General Message
ICS 215	Operational Planning Worksheet

Table A-3—ICS Forms that Can Aid the Planning Process

TAB 9—EXAMPLES OF ICS FORMS

The following pages contain examples of the ICS Forms that are discussed in this document. These examples have been drawn from the U.S. Department of Agriculture's Forest Service; other emergency management organizations also provide ICS hardcopy forms and software packages to generate ICS forms that may be used for incident management purposes.

Number	Purpose
ICS 201 (p.1)	Incident Briefing
ICS 201 (p.2)	Summary of Current Actions
ICS 202	Incident Objectives
ICS 203	Organization Assignment List
ICS 204	Assignment List
ICS 205	Incident Radio Communications Plan
ICS 206	Medical Plan
ICS 215	Operational Planning Worksheet

Table A-4—Examples of ICS Forms Included in this Tab

(This Page Intentionally Left Blank)

INCIDENT BRIEFING	1. Incident Name	2. Date	3. Time

4. Map Sketch

5. Current Organization

Incident Commander

Safety Officer

Liaison Officer or Agency Rep:

Information Officer:

Planning	Operations	Logistics	Finance
Div _____	Div _____	Div _____	Div _____

Air

Air Operations _____

Air Support _____

Air Attack _____

Air Tanker Coord _____

Helicopter Coord _____

Page 1 of	6. Prepared by (Name and Position)

6. Resources Summary			
Resources Ordered	Resource Identification	ETA On Scene	Location/Assignment

7. Summary of Current Actions

Page 2 of	

INCIDENT OBJECTIVES	1. Incident Name	2. Date	3. Time

4. Operational Period

5. General Control Objectives for the Incident (include alternatives)

6. Weather Forecast for Period

7. General Safety Message

8. Attachments (mark if attached)

☐ Organization List - ICS 203	☐ Medical Plan - ICS 206	☐ (Other)
☐ Div. Assignment Lists - ICS 204	☐ Incident Map	☐
☐ Communications Plan - ICS 205	☐ Traffic Plan	☐

9. Prepared by (Planning Section Chief)	10. Approved by (Incident Commander)

ICS 202

(This Page Intentionally Left Blank)

ORGANIZATION ASSIGNMENT LIST

1. Incident Name	
2. Date	3. Time
4. Operational Period	

Position	Name
5. Incident Commander and Staff	
Incident Commander	
Deputy	
Safety Officer	
Information Officer	
Liaison Officer	
6. Agency Representative	
Agency	Name
7. Planning Section	
Chief	
Deputy	
Resources Unit	
Situation Unit	
Documentation Unit	
Demobilization Unit	
Technical Specialists	
Human Resources	
Training	
8. Logistics Section	
Chief	
Deputy	
Supply Unit	
Facilities Unit	
Ground Support Unit	
Communications Unit	
Medical Unit	
Security Unit	
Food Unit	

9. Operations Section		
Chief		
Deputy		
a. Branch I - Division/Groups		
Branch Director		
Deputy		
Division/Group		
Division/Group		
Division/Group		
Division/Group		
Division/Group		
b. Branch II - Division/Groups		
Branch Director		
Deputy		
Division/Group		
Division/Group		
Division/Group		
Division/Group		
Division/Group		
c. Branch III - Division/Groups		
Branch Director		
Deputy		
Division/Group		
Division/Group		
Division/Group		
Division/Group		
Division/Group		
d. Air Operations Branch		
Air Operations Branch Director		
Air Attack Supervisor		
Air Support Supervisor		
Helicopter Coordinator		
Air Tanker Coordinator		
10. Finance Section		
Chief		
Deputy		
Time Unit		
Procurement Unit		
Compensation/Claims Unit		
Cost Unit		

Prepared by (Resource Unit Leader)

(This Page Intentionally Left Blank)

DIVISION ASSIGNMENT LIST	1. Branch	2. Division/Group
3. Incident Name	4. Operational Period Date: Time:	

5. Operations Personnel

Operations Chief		Division/Group Supervisor	
Branch Director		Air Attack Supervisor No	

6. Resources Assigned this Period

Strike Team/Task Force/ Resource Designator	Leader	Number Persons	Trans. Needed	Drop Off PT /Time	Pick Up PT /Time

7. Control Operations

8. Special Instructions

9. Division/Group Communication Summary

Function	Frequency	System	Channel	Function	Frequency	System	Channel
Command		King NBC		Logistics		King NBC	
Tactical Div/Group		King NBC		Air to/Ground		King NBC	

Prepared by (Resource Unit Leader)	Approved by (Planning Section Chief)	Date	Time

(This Page Intentionally Left Blank)

INCIDENT RADIO COMMUNICATIONS PLAN	1. Incident Name	2. Date/Time Prepared	3. Operational Period Date/Time

4. Basic Radio Channel Utilization

Radio Type/Cache	Channel	Function	Frequency/Tone	Assignment	Remarks
King NIFC					
King NIFC					
King NIFC					
King NIFC					
King NIFC					
King NIFC					
King NIFC					
King NIFC					

5. Prepared by (Communications Unit)

(This Page Intentionally Left Blank)

MEDICAL PLAN	1. Incident Name	2. Date Prepared	3. Time Prepared	4. Operational Period

5. Incident Medical Aid Station

Medical Aid Stations	Location	Paramedics Yes	No

6. Transportation

A. Ambulance Services

Name	Address	Phone	Paramedics Yes	No

B. Incident Ambulances

Name	Location	Paramedics Yes	No

7. Hospitals

Name	Address	Travel Time Air	Ground	Phone	Helipad Yes	No	Burn Center Yes	No

8. Medical Emergency Procedures

Prepared by (Medical Unit Leader)	10. Reviewed by (Safety Officer)

ICS 206

(This Page Intentionally Left Blank)

OPERATIONAL PLANNING WORK SHEET

Incident Name:

2. Date Prepared

Time Prepared

3. Operational Period (Date/Time)

1. Division/Group or Other	2.		Resource by Type (Show Strike Teams as ST)																			6. Reporting Locations	7. Requested Arrival Time
Location	Work Assignments		Engines				Water Tenders		Hand Crews		Dozers			Helicopters				Air Tankers			Other		
			1	2	3	4	1	2	1	2	1	2	3	1	2	3	4	1	2	3			
		Req																					
		Have																					
		Need																					
		Req																					
		Have																					
		Need																					
		Req																					
		Have																					
		Need																					
		Req																					
		Have																					
		Need																					
		Req																					
		Have																					
		Need																					
		Req																					
		Have																					
		Need																					
8. Total Resources - Single		Req																					
		Have																					
		Need																					
Total Resources - Strike Teams		Req																				Prepared By (Name and Position)	
		Have																					
		Need																					

NFES 1338

ICS 215

(This Page Intentionally Left Blank)

APPENDIX B

NATIONAL INCIDENT MANAGEMENT RESOURCE TYPING SYSTEM

A. PURPOSE.

This appendix provides additional information regarding the national equipment typing system specified in Chapter IV of this document.

B. RESPONSIBLITIES.

The NIMS Integration Center described in Chapter VII has the overall responsibility for ongoing development and refinement of various NIMS activities and programs. Under its auspices, the National Resource Management Working Group, chaired by the Emergency Preparedness and Response Directorate of the Department of Homeland Security, is responsible for establishing a national resource typing protocol. The NIMS resource typing protocol is based on inputs from representatives from various Federal agencies and departments and private organizations, as well as representatives of State and local emergency management; law enforcement; firefighting and emergency medical services; public health; public works; and other entities with assigned responsibilities under the Federal Response Plan and the National Response Plan. Federal, State, local, and tribal authorities should use the national typing protocol when inventorying and managing resources to promote common interoperability and integration.

C. ELEMENTS OF THE NATIONAL TYPING PROTOCOL

The resource typing protocol provided by the NIMS describes resources using category, kind, components, metrics, and type data. The following data definitions will be used:

1. Resource

For purposes of typing, *resources* consist of personnel, teams, facilities, supplies, and major items of equipment available for assignment to or use during incidents. Such resources may be used in tactical support or supervisory capacities at an incident site or EOC. Their descriptions include category, kind, components, metrics, and type.

2. Category

A *category* is the function for which a resource would be most useful. Table B-1 briefly describes the categories used in the national resource typing protocol.

Category	Purpose
Transportation	To assist Federal agencies, State and local governments, and voluntary organizations requiring transportation to perform incident management missions following a major disaster or emergency; to coordinate incident management operations and restoration of the transportation infrastructure
Communications	To provide communications support for Federal, State, local, and tribal incident management efforts
Public works and engineering	To assist those engaged in lifesaving, life-sustaining, damage mitigation, and recovery operations following a major disaster or emergency by providing technical advice, evaluation, and engineering services; by contracting for construction management and inspection and for the emergency repair of water and wastewater treatment facilities; supplying potable water and ice and emergency power; and arranging for needed real estate.
Firefighting	To detect and suppress urban, suburban, and rural fires.
Information and planning	To collect, analyze, process, and disseminate information about a potential or actual disaster or emergency to facilitate overall activities in providing assistance to support planning and decision-making.
Law enforcement and security	To provide law enforcement assistance during response and recovery operations; to assist with site security and investigation.
Mass care	To support efforts to meet the mass care needs of disaster victims including delivering such services as supplying victims with shelter, feeding, and emergency first aid; supplying bulk distribution of emergency relief supplies; and collecting information to and for a disaster welfare information system designed to report on victim status and assist in reuniting families.
Resource management	To provide operational assistance for incident management operations.
Health and medical	To provide assistance to supplement local resources in meeting public health and medical care needs following a disaster or emergency or during a potential developing medical situation.
Search and rescue	To provide specialized lifesaving assistance in the event of a disaster or emergency, including locating, extricating, and providing on-site medical treatment to victims trapped in collapsed structures.
Hazardous materials response	To support the response to an actual or potential discharge and/or release of hazardous materials.
Food and water	To identify, secure, and arrange for the transportation of safe food and water to affected areas during a disaster or emergency.
Energy	To help restore energy systems following a disaster or emergency.
Public information	To contribute to the well-being of the community following a disaster by disseminating accurate, consistent, timely, and easy-to-understand information; to gather and disseminate information about disaster response and recovery process.
Animals and agricultural issues	To coordinate activities responding to an agricultural disaster and/or when the health or care of animals is at issue.
Volunteers and donations	To support the management of unsolicited goods and unaffiliated volunteers, and to help establish a system for managing and controlling donated goods and services.

Table B-1—Categories Used in the National Resource Typing System

3. Kind

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

4. Components

Resources can comprise multiple *components*. For example, an engine company may be listed as having the eight components shown in Table B-2.

(1) Pump	(5) Water tank
(2) Hose 2 __"	(6) Ladder
(3) Hose 1 __"	(7) Master Stream
(4) Hose 1"	(8) Personnel

Table B-2—Example of a Resource with Multiple Components (Fire Fighting Engine Company)

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

5. Metrics

Metrics are measurement standards. The metrics used will differ depending on the kind of resource being typed. The mission envisioned determines the specific metric selected. The metric must be useful in describing a resource's capability to support the mission. As an example, one metric for a disaster medical assistance team is the number of patients it can care for per day. Likewise, an appropriate metric for a hose might be the number of gallons of water per hour that can flow through it. Metrics should identify capability and/or capacity.

6. Type

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

resource. For example, the U.S. Coast Guard has typed oil skimmers based on barrels per day, as outlined below in Table B-3:

Type I	9,600 bbls/day	Type III	480 bbls/day
Type II	2,880 bbls/day	Type IV	N/A

Table B-3—Example of a Resource with Multiple Types (Coast Guard Oil Skimmer)

7. Additional Information

The national resource typing protocol will also provide the capability to use additional information that is pertinent to resource decision-making. For example, if a particular set of resources can only be released to support an incident under particular authorities or laws, the protocol should provide the ability for resource managers to understand such limitations.

D. EXAMPLE OF A RESOURCE FOR WHICH TYPING HAS BEEN COMPLETED

As an illustration of how the national equipment typing system is used, Figure B-4 is an example of a resource that has been completely typed, an urban search and rescue task force.

Resource: Urban Search & Rescue (US&R) Task Forces					
Category:		Search and Rescue		Kind:	Team
Minimum Capabilities:		Type I	Type II	Type III	Type IV
Component	Metric				
Personnel	Number of People per Response	70 person response	28 person response		
Personnel	Training	NFPA 1670 Technician Level in area of specialty. Support personnel at Operations Level.	NFPA 1670 Technician Level in area of specialty. Support personnel at Operations Level.		
Personnel	Areas of specialization	High angle rope rescue (including highline systems); confined space rescue (permit required); Advanced Life Support (ALS) intervention; communications; WMD/HM operations; defensive water rescue	Light frame construction and basic rope rescue operations; ALS intervention; HazMat conditions; communications; and trench and excavation rescue		
Personnel	Sustained Operations	24-hour S&R operations. Self-sufficient for first 72 hours.	12-hour S&R operations. Self-sufficient for first 72 hours.		
Personnel	Organization	Multi-disciplinary organization of Command, Search, Rescue, Medical, HazMat, Logistics, and Planning.	Multi-disciplinary organization of Command, Search, Rescue, Medical, HazMat, Logistics, and Planning.		
Equipment	Sustained Operations	Potential mission duration of up to 10 days.	Potential mission duration of up to 10 days.		
Equipment	Rescue Equipment	Pneumatic Powered Tools, Electric Powered Tools, Hydraulic Powered Tools, Hand Tools, Electrical, Heavy Rigging, Technical Rope, Safety	Pneumatic Powered Tools, Electric Powered Tools, Hydraulic Powered Tools, Hand Tools, Electrical, Heavy Rigging, Technical Rope, Safety		
Equipment	Medical Equipment	Antibiotics/ Antifungals, Patient Comfort Medication, Pain Medications, Sedatives/ Anesthetics/ Paralytics, Steroids, IV Fluids/ Volume, Immunizations/ Immune Globulin, Canine Treatment, Basic Airway, Intubation, Eye Care Supplies, IV Access/ Administration, Patient Assessment Care, Patient Immobilization/ Extrication, Patient/ PPE, Skeletal Care, Wound Care, Patient Monitoring	Antibiotics/ Antifungals, Patient Comfort Medication, Pain Medications, Sedatives/ Anesthetics/ Paralytics, Steroids, IV Fluids/ Volume, Immunizations/ Immune Globulin, Canine Treatment, Basic Airway, Intubation, Eye Care Supplies, IV Access/ Administration, Patient Assessment Care, Patient Immobilization/ Extrication, Patient/ PPE, Skeletal Care, Wound Care, Patient Monitoring		
Equipment	Technical Equipment	Structures Specialist Equip, Technical Information Specialist Equip, HazMat Specialist Equip, Technical Search Specialist Equip, Canine Search Specialist Equip	Structures Specialist Equip, Technical Information Specialist Equip, HazMat Specialist Equip, Technical Search Specialist Equip, Canine Search Specialist Equip		
Equipment	Communications Equipment	Portable Radios, Charging Units, Telecommunications, Repeaters, Accessories, Batteries, Power Sources, Small Tools, Computer	Portable Radios, Charging Units, Telecommunications, Repeaters, Accessories, Batteries, Power Sources, Small Tools, Computer		
Equipment	Logistics Equipment	Water/Fluids, Food, Shelter, Sanitation, Safety, Administrative Support, Personal Bag, Task Force Support, Cache Transportation/ Support, Base of Operations, Equipment Maintenance	Water/Fluids, Food, Shelter, Sanitation, Safety, Administrative Support, Personal Bag, Task Force Support, Cache Transportation/ Support, Base of Operations, Equipment Maintenance		
Comments		Federal asset. There are 28 FEMA US&R Task Forces, totally self-sufficient for the first 72 hours of a deployment, spread throughout the continental United States trained and equipped by FEMA to conduct physical search-and-rescue in collapsed buildings, provide emergency medical care to trapped victims, assess and control gas, electrical services and hazardous materials, and evaluate and stabilize damaged structures.			

Table B-4—Example of a Fully Typed Resource (Urban Search and Rescue Task Forces)

(This Page Intentionally Left Blank)

GLOSSARY OF KEY TERMS

For the purposes of the NIMS, the following terms and definitions apply:

Agency: A division of government with a specific function offering a particular kind of assistance. In ICS, agencies are defined either as jurisdictional (having statutory responsibility for incident management) or as assisting or cooperating (providing resources or other assistance).

Agency Representative: A person assigned by a primary, assisting, or cooperating Federal, State, local, or tribal government agency or private entity that has been delegated authority to make decisions affecting that agency's or organization's participation in incident management activities following appropriate consultation with the leadership of that agency.

Area Command (Unified Area Command): An organization established (1) to oversee the management of multiple incidents that are each being handled by an ICS organization or (2) to oversee the management of large or multiple incidents to which several Incident Management Teams have been assigned. Area Command has the responsibility to set overall strategy and priorities, allocate critical resources according to priorities, ensure that incidents are properly managed, and ensure that objectives are met and strategies followed. Area Command becomes Unified Area Command when incidents are multijurisdictional. Area Command may be established at an emergency operations center facility or at some location other than an incident command post.

Assessment: The evaluation and interpretation of measurements and other information to provide a basis for decision-making.

Assignments: Tasks given to resources to perform within a given operational period that are based on operational objectives defined in the IAP.

Assistant: Title for subordinates of principal Command Staff positions. The title indicates a level of technical capability, qualifications, and responsibility subordinate to the primary positions. Assistants may also be assigned to unit leaders.

Assisting Agency: An agency or organization providing personnel, services, or other resources to the agency with direct responsibility for incident management. See also Supporting Agency.

Available Resources: Resources assigned to an incident, checked in, and available for a mission assignment, normally located in a Staging Area.

Branch: The organizational level having functional or geographical responsibility for major aspects of incident operations. A branch is organizationally situated between the section and the division or group in the Operations Section, and between the section and

units in the Logistics Section. Branches are identified by the use of Roman numerals or by functional area.

Chain of Command: A series of command, control, executive, or management positions in hierarchical order of authority.

Check-In: The process through which resources first report to an incident. Check-in locations include the incident command post, Resources Unit, incident base, camps, staging areas, or directly on the site.

Chief: The ICS title for individuals responsible for management of functional sections: Operations, Planning, Logistics, Finance/Administration, and Intelligence (if established as a separate section).

Command: The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority.

Command Staff: In an incident management organization, the Command Staff consists of the Incident Command and the special staff positions of Public Information Officer, Safety Officer, Liaison Officer, and other positions as required, who report directly to the Incident Commander. They may have an assistant or assistants, as needed.

Common Operating Picture: A broad view of the overall situation as reflected by situation reports, aerial photography, and other information or intelligence.

Communications Unit: An organizational unit in the Logistics Section responsible for providing communication services at an incident or an EOC. A Communications Unit may also be a facility (e.g., a trailer or mobile van) used to support an Incident Communications Center.

Cooperating Agency: An agency supplying assistance other than direct operational or support functions or resources to the incident management effort.

Coordinate: To advance systematically an analysis and exchange of information among principals who have or may have a need to know certain information to carry out specific incident management responsibilities.

Deputy: A fully qualified individual who, in the absence of a superior, can be delegated the authority to manage a functional operation or perform a specific task. In some cases, a deputy can act as relief for a superior and, therefore, must be fully qualified in the position. Deputies can be assigned to the Incident Commander, General Staff, and Branch Directors.

Dispatch: The ordered movement of a resource or resources to an assigned operational mission or an administrative move from one location to another.

Division: The partition of an incident into geographical areas of operation. Divisions are established when the number of resources exceeds the manageable span of control of the Operations Chief. A division is located within the ICS organization between the branch and resources in the Operations Section.

Emergency: Absent a Presidentially declared emergency, any incident(s), human-caused or natural, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.

Emergency Operations Centers (EOCs): The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or some combination thereof.

Emergency Operations Plan: The "steady-state" plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards.

Emergency Public Information: Information that is disseminated primarily in anticipation of an emergency or during an emergency. In addition to providing situational information to the public, it also frequently provides directive actions required to be taken by the general public.

Emergency Response Provider: Includes Federal, State, local, and tribal emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities. See Section 2 (6), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002). Also known as *Emergency Responder.*

Evacuation: Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

Event: A planned, nonemergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.

Federal: Of or pertaining to the Federal Government of the United States of America.

Function: Function refers to the five major activities in ICS: Command, Operations, Planning, Logistics, and Finance/Administration. The term function is also used when describing the activity involved, e.g., the planning function. A sixth function, Intelligence, may be established, if required, to meet incident management needs.

General Staff: A group of incident management personnel organized according to function and reporting to the Incident Commander. The General Staff normally consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief.

Group: Established to divide the incident management structure into functional areas of operation. Groups are composed of resources assembled to perform a special function not necessarily within a single geographic division. Groups, when activated, are located between branches and resources in the Operations Section. (See *Division.*)

Hazard: Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Incident: An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Incident Action Plan: An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods.

Incident Command Post (ICP): The field location at which the primary tactical-level, on-scene incident command functions are performed. The ICP may be collocated with the incident base or other incident facilities and is normally identified by a green rotating or flashing light.

Incident Command System (ICS): A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small as well as large and complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations.

Incident Commander (IC): The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

Incident Management Team (IMT): The IC and appropriate Command and General Staff personnel assigned to an incident.

Incident Objectives: Statements of guidance and direction necessary for selecting appropriate strategy(s) and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources

have been effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow strategic and tactical alternatives.

Initial Action: The actions taken by those responders first to arrive at an incident site.

Initial Response: Resources initially committed to an incident.

Intelligence Officer: The intelligence officer is responsible for managing internal information, intelligence, and operational security requirements supporting incident management activities. These may 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, law enforcement sensitive information, proprietary 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 to perform their missions effectively and safely.

Joint Information Center (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media at the scene of the incident. Public information officials from all participating agencies should collocate at the JIC.

Joint Information System (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, timely information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated interagency messages; developing, recommending, and executing public information plans and strategies on behalf of the IC; advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.

Jurisdiction: A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health).

Liaison: A form of communication for establishing and maintaining mutual understanding and cooperation.

Liaison Officer: A member of the Command Staff responsible for coordinating with representatives from cooperating and assisting agencies.

Local Government: 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; a rural community, unincorporated town

or village, or other public entity. See Section 2 (10), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Logistics: Providing resources and other services to support incident management.

Logistics Section: The section responsible for providing facilities, services, and material support for the incident.

Major Disaster: As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is

> any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, tribes, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Management by Objective: A management approach that involves a four-step process for achieving the incident goal. The Management by Objectives 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 fulfill them, in support of defined strategic objectives; and documenting results to measure performance and facilitate corrective action.

Mitigation: The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

Mobilization: The process and procedures used by all organizations—Federal, State, local, and tribal—for activating, assembling, and transporting all resources that have been requested to respond to or support an incident.

Multiagency Coordination Entity: A multiagency coordination entity functions within a broader multiagency coordination system. It may establish the priorities among incidents and associated resource allocations, deconflict agency policies, and provide strategic guidance and direction to support incident management activities.

Multiagency Coordination Systems: Multiagency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The components of multiagency coordination systems include facilities, equipment, emergency operation centers (EOCs), specific multiagency coordination entities, personnel, procedures, and communications. These systems assist agencies and organizations to fully integrate the subsystems of the NIMS.

Multijurisdictional Incident: An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under Unified Command.

Mutual-Aid Agreement: Written agreement between agencies and/or jurisdictions that they will assist one another on request, by furnishing personnel, equipment, and/or expertise in a specified manner.

National: Of a nationwide character, including the Federal, State, local, and tribal aspects of governance and polity.

National Disaster Medical System: A cooperative, asset-sharing partnership between the Department of Health and Human Services, the Department of Veterans Affairs, the Department of Homeland Security, and the Department of Defense. NDMS provides resources for meeting the continuity of care and mental health services requirements of the Emergency Support Function 8 in the Federal Response Plan.

National Incident Management System: A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and tribal governments; the private-sector, and nongovernmental organizations 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 among Federal, State, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multiagency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

National Response Plan: A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.

Nongovernmental Organization: An entity with an association that is based on interests of its members, individuals, or institutions and that is not created by a government, but may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross.

Operational Period: The time scheduled for executing a given set of operation actions, as specified in the Incident Action Plan. Operational periods can be of various lengths, although usually not over 24 hours.

Operations Section: The section responsible for all tactical incident operations. In ICS, it normally includes subordinate branches, divisions, and/or groups.

Personnel Accountability: The ability to account for the location and welfare of incident personnel. It is accomplished when supervisors ensure that ICS principles and processes are functional and that personnel are working within established incident management guidelines.

Planning Meeting: A meeting held as needed prior to and throughout the duration of an incident to select specific strategies and tactics for incident control operations and for service and support planning. For larger incidents, the planning meeting is a major element in the development of the Incident Action Plan (IAP).

Planning Section: Responsible for the collection, evaluation, and dissemination of operational information related to the incident, and for the preparation and documentation of the IAP. This section also maintains information on the current and forecasted situation and on the status of resources assigned to the incident.

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.

Preparedness Organizations: The groups and fora that provide interagency coordination for domestic incident management activities in a nonemergency context. Preparedness organizations can include all agencies with a role in incident management, for prevention, preparedness, response, or recovery activities. They represent a wide variety of committees, planning groups, and other organizations that meet and coordinate to ensure the proper level of planning, training, equipping, and other preparedness requirements within a jurisdiction or area.

Prevention: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at

deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Private Sector: Organizations and entities that are not part of any governmental structure. It includes for-profit and not-for-profit organizations, formal and informal structures, commerce and industry, and private voluntary organizations (PVO).

Processes: Systems of operations that incorporate standardized procedures, methodologies, and functions necessary to provide resources effectively and efficiently. These include resource typing, resource ordering and tracking, and coordination.

Public Information Officer: A member of the Command Staff responsible for interfacing with the public and media or with other agencies with incident-related information requirements.

Publications Management: The publications management subsystem includes materials development, publication control, publication supply, and distribution. The development and distribution of NIMS materials is managed through this subsystem. Consistent documentation is critical to success, because it ensures that all responders are familiar with the documentation used in a particular incident regardless of the location or the responding agencies involved.

Qualification and Certification: This subsystem provides recommended qualification and certification standards for emergency responder and incident management personnel. It also allows the development of minimum standards for resources expected to have an interstate application. Standards typically include training, currency, experience, and physical and medical fitness.

Reception Area: This refers to a location separate from staging areas, where resources report in for processing and out-processing. Reception Areas provide accountability, security, situational awareness briefings, safety awareness, distribution of IAPs, supplies and equipment, feeding, and bed down.

Recovery: The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; postincident reporting; and development of initiatives to mitigate the effects of future incidents.

Recovery Plan: A plan developed by a State, local, or tribal jurisdiction with assistance from responding Federal agencies to restore the affected area.

Resources: Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC.

Resource Management: Efficient incident management requires a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. Resource management under the NIMS includes mutual-aid agreements; the use of special Federal, State, local, and tribal teams; and resource mobilization protocols.

Resources Unit: Functional unit within the Planning Section responsible for recording the status of resources committed to the incident. This unit also evaluates resources currently committed to the incident, the effects additional responding resources will have on the incident, and anticipated resource needs.

Response: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Safety Officer: A member of the Command Staff responsible for monitoring and assessing safety hazards or unsafe situations and for developing measures for ensuring personnel safety.

Section: The organizational level having responsibility for a major functional area of incident management, e.g., Operations, Planning, Logistics, Finance/Administration, and Intelligence (if established). The section is organizationally situated between the branch and the Incident Command.

Span of Control: The number of individuals a supervisor is responsible for, usually expressed as the ratio of supervisors to individuals. (Under the NIMS, an appropriate span of control is between 1:3 and 1:7.)

Staging Area: Location established where resources can be placed while awaiting a tactical assignment. The Operations Section manages Staging Areas.

State: When capitalized, refers to 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. See Section 2 (14), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Strategic: Strategic elements of incident management are characterized by continuous long-term, high-level planning by organizations headed by elected or other senior officials. These elements involve the adoption of long-range goals and objectives, the

setting of priorities; the establishment of budgets and other fiscal decisions, policy development, and the application of measures of performance or effectiveness.

Strike Team: A set number of resources of the same kind and type that have an established minimum number of personnel.

Strategy: The general direction selected to accomplish incident objectives set by the IC.

Supporting Technologies: Any technology that may be used to support the NIMS is included in this subsystem. These technologies include orthophoto mapping, remote automatic weather stations, infrared technology, and communications, among various others.

Task Force: Any combination of resources assembled to support a specific mission or operational need. All resource elements within a Task Force must have common communications and a designated leader.

Technical Assistance: Support provided to State, local, and tribal jurisdictions when they have the resources but lack the complete knowledge and skills needed to perform a required activity (such as mobile-home park design and hazardous material assessments).

Terrorism: Under the Homeland Security Act of 2002, terrorism is defined as activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources and is a violation of the criminal laws of the United States or of any State or other subdivision of the United States in which it occurs and is intended to intimidate or coerce the civilian population or influence a government or affect the conduct of a government by mass destruction, assassination, or kidnapping. See Section 2 (15), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Threat: An indication of possible violence, harm, or danger.

Tools: Those instruments and capabilities that allow for the professional performance of tasks, such as information systems, agreements, doctrine, capabilities, and legislative authorities.

Tribal: Any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaskan Native Claims Settlement Act (85 stat. 688) [43 U.S.C.A. and 1601 et seq.], that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

Type: A classification of resources in the ICS that refers to capability. Type 1 is generally considered to be more capable than Types 2, 3, or 4, respectively, because of size; power; capacity; or, in the case of incident management teams, experience and qualifications.

Unified Area Command: A Unified Area Command is established when incidents under an Area Command are multijurisdictional. (See *Area Command.*)

Unified Command: An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP.

Unit: The organizational element having functional responsibility for a specific incident planning, logistics, or finance/administration activity.

Unity of Command: The concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.

Volunteer: For purposes of the NIMS, a volunteer is any individual accepted to perform services by the lead agency, which has authority to accept volunteer services, when the individual performs services without promise, expectation, or receipt of compensation for services performed. See, e.g., 16 U.S.C. 742f(c) and 29 CFR 553.101.

ACRONYMS

ALS	Advanced Life Support
DOC	Department Operations Center
EMAC	Emergency Management Assistance Compact
EOC	Emergency Operations Center
EOP	Emergency Operations Plan
FOG	Field Operations Guide
GIS	Geographic Information System
HAZMAT	Hazardous Material
HSPD-5	Homeland Security Presidential Directive-5
IAP	Incident Action Plan
IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IC or UC	Incident Command or Unified Command
IMT	Incident Management Team
JIS	Joint Information System
JIC	Joint Information Center
LNO	Liaison Officer
NDMS	National Disaster Medical System
NGO	Nongovernmental Organization
NIMS	National Incident Management System
NRP	National Response Plan
POLREP	Pollution Report
PIO	Public Information Officer
PVO	Private Voluntary Organizations
R&D	Research and Development
RESTAT	Resources Status
ROSS	Resource Ordering and Status System
SDO	Standards Development Organizations
SITREP	Situation Report
SO	Safety Officer
SOP	Standard Operating Procedure
UC	Unified Command
US&R	Urban Search and Rescue

(This Page Intentionally Left Blank)