National Incident Management System

Third Edition
October 2017

FEMA

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

Homeland Security

October 10, 2017

Dear National Incident Management System Community:

Originally issued in 2004, the National Incident Management System (NIMS) provides a consistent nationwide template to enable partners across the Nation to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity.

Since the Federal Emergency Management Agency (FEMA) last revised the NIMS guidance in 2008, the risk environment has evolved, and our national incident management capabilities have matured. This revision incorporates lessons learned and best practices from a wide variety of disciplines, at all levels of government, from the private sector, tribes, and nongovernmental organizations.

The FEMA Administrator, in his role as the head of the National Integration Center, is charged with managing and maintaining NIMS, and in accordance with the Post-Katrina Emergency Management Reform Act, will issue the revised NIMS guidance and support its implementation.

I believe this revised version of NIMS advances our national preparedness and takes us collectively into the future of incident management.

Sincerely,

Elaine C. Duke
Acting Secretary

U.S. Department of Homeland Security
Washington, DC 20472

FEMA

October 10, 2017

Dear NIMS Community:

Since the Department of Homeland Security first published the National Incident Management System (NIMS) in 2004, our Nation has made great strides in working together before, during, and after emergencies and planned events. Every day, men and women from a wide variety of organizations work together to save lives and protect property and the environment. This national unity of effort strengthens organizations across the whole community by enabling them to share resources and help one another in times of need.

To keep NIMS guidance pertinent, accurate, and up-to-date, FEMA engaged partners and practitioners from a wide variety of disciplines, at all levels of government, from the private sector, tribes, and nongovernmental organizations. This document retains much of the material from the 2008 version of NIMS. It synchronizes the guidance with changes to laws, policies, and best practices, and adds information on the roles of off-scene incident personnel, including senior leaders and staff in emergency operations centers.

Perhaps more than any other homeland security guidance, NIMS has always been, and continues to be, the product of practitioners, based on the experience of emergency personnel who respond to incidents every day. As NIMS continues to mature, its purpose remains the same: to enhance unity of effort by providing a common approach for managing incidents. I believe that this document advances that cause and I am pleased to approve and endorse this revised version of NIMS.

Sincerely,

Brock Long
Administrator

Contents

I. Fundamentals and Concepts of NIMS

A. Introduction

Communities across the Nation experience a diverse set of threats, hazards, and events. The size, frequency, complexity, and scope of these incidents[1] vary, but all involve a range of personnel and organizations to coordinate efforts to save lives, stabilize the incident, and protect property and the environment. Every day, jurisdictions and organizations work together to share resources, integrate tactics, and act collaboratively. Whether these organizations are nearby or are supporting each other from across the country, their success depends on a common, interoperable approach to sharing resources, coordinating and managing incidents, and communicating information. The National Incident Management System (NIMS) defines this comprehensive approach.

NIMS guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides stakeholders across the whole community[2] with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System.[3] NIMS defines operational systems, including the Incident Command System (ICS), Emergency Operations Center (EOC) structures, and Multiagency Coordination Groups (MAC Groups) that guide how personnel work together during incidents. NIMS applies to all incidents, from traffic accidents to major disasters.

The jurisdictions and organizations involved in managing incidents vary in their authorities, management structures, communication capabilities and protocols, and many other factors. NIMS provides a common framework to integrate these diverse capabilities and achieve common goals. The guidance contained in this document incorporates solutions developed over decades of experience by incident personnel across the Nation.

This document is organized into three major components:

- **Resource Management** describes standard mechanisms to systematically manage resources, including personnel, equipment, supplies, teams, and facilities, both before and during incidents in order to allow organizations to more effectively share resources when needed.

[1] In this document, the word "incident" includes planned events as well as emergencies and/or disasters of all kinds and sizes. See the Glossary for additional information.
[2] Whole community is a focus on enabling the participation in incident management activities of a wider range of players from the private and nonprofit sectors, including NGOs and the general public, in conjunction with the participation of all levels of government in order to foster better coordination and working relationships.
[3] The National Preparedness System outlines an organized process to help the whole community achieve the National Preparedness Goal. It comprises and builds on existing policies, programs, and guidance to include the National Planning Frameworks, Federal Interagency Operational Plans, and the National Preparedness Report.

- **Command and Coordination** describes leadership roles, processes, and recommended organizational structures for incident management at the operational and incident support levels and explains how these structures interact to manage incidents effectively and efficiently.
- **Communications and Information Management** describes systems and methods that help to ensure that incident personnel and other decision makers have the means and information they need to make and communicate decisions.

These components represent a building-block approach to incident management. Applying the guidance for all three components is vital to successful NIMS implementation.

B. Applicability and Scope

NIMS is applicable to all stakeholders with incident management and support responsibilities. The audience for NIMS includes emergency responders and other emergency management personnel, NGOs (e.g., faith-based and community-based groups), the private sector, and elected and appointed officials responsible for making decisions regarding incidents. All incident management efforts, regardless of the incident or location, should fully incorporate people with disabilities and other people who have access and functional needs.[4] The scope of NIMS includes all incidents, regardless of size, complexity, or scope, and planned events (e.g., sporting events). Table 1 describes the utility of NIMS as incident management doctrine.

Table 1: Overview of NIMS

NIMS Is	NIMS Is Not
• A comprehensive, nationwide, systematic approach to incident management, including the command and coordination of incidents, resource management, and information management	• Only the ICS • Only applicable to certain emergency/incident response personnel • A static system
• A set of concepts and principles for all threats, hazards, and events across all mission areas (Prevention, Protection, Mitigation, Response, Recovery)	• A response plan
• Scalable, flexible, and adaptable; used for all incidents, from day-to-day to large-scale	• Used only during large-scale incidents
• Standard resource management procedures that enable coordination among different jurisdictions or organizations	• A resource-ordering system
• Essential principles for communications and information management	• A communications plan

[4] Access and functional needs are individual circumstances requiring assistance, accommodation, or modification for mobility, communication, transportation, safety, health maintenance, etc., due to any temporary or permanent situation that limits an individual's ability to take action during an incident.

C. NIMS Guiding Principles

Incident management priorities include saving lives, stabilizing the incident, and protecting property and the environment. To achieve these priorities, incident personnel apply and implement NIMS components in accordance with the principles of flexibility, standardization, and unity of effort.

Flexibility

NIMS components are adaptable to any situation, from planned special events to routine local incidents to incidents involving interstate mutual aid or Federal assistance. Some incidents need multiagency, multijurisdictional, and/or multidisciplinary coordination. Flexibility allows NIMS to be scalable and, therefore, applicable for incidents that vary widely in terms of hazard, geography, demographics, climate, cultural, and organizational authorities.

Standardization

Standardization is essential to interoperability among multiple organizations in incident response. NIMS defines standard organizational structures that improve integration and connectivity among jurisdictions and organizations. NIMS defines standard practices that allow incident personnel to work together effectively and foster cohesion among the various organizations involved. NIMS also includes common terminology, which enables effective communication.

Unity of Effort

Unity of effort means coordinating activities among various organizations to achieve common objectives. Unity of effort enables organizations with specific jurisdictional responsibilities to support each other while maintaining their own authorities.

D. Background

NIMS is the culmination of more than 40 years of efforts to improve interoperability in incident management. This work began in the 1970s with local, state,[5] and Federal agencies collaborating to create a system called Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE). FIRESCOPE included ICS and the Multiagency Coordination System (MACS). In 1982, the agencies that developed FIRESCOPE and the National Wildfire Coordinating Group (NWCG) created the National Interagency Incident Management System (NIIMS), in part to make ICS and MACS guidance applicable to all types of incidents and all hazards. Recognizing the value of these systems, communities across the Nation adopted ICS and MACS, but adoption was not universal.

In the aftermath of the 2001 terrorist attacks, the need for an integrated nationwide incident management system with standard structures, terminology, processes, and resources became

[5] In this document, "state" refers to the 56 states, territories, and insular areas (which includes any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands).

clear. The Department of Homeland Security (DHS) led a national effort to consolidate, expand, and enhance the previous work of FIRESCOPE, NIIMS, and others to develop NIMS.

The Federal Emergency Management Agency (FEMA) published the first NIMS document in 2004 and revised it in 2008. This 2017 version reflects progress since 2008, based on lessons learned, best practices, and changes in national policy, including updates to the National Preparedness System. Additionally, this version:

- Reiterates concepts and principles of the earlier versions of NIMS;
- Provides additional guidance for EOCs; and
- Describes how NIMS command and coordination mechanisms fit together.

E. Key Terms

Several key terms are used throughout this document. While described in greater detail in the Resource Management Component, Command and Coordination Component, and supporting appendices, it is important to define these terms up front.

Area Command: When very complex incidents, or multiple concurrent smaller incidents, require the establishment of multiple ICS organizations, an Area Command can be established to oversee their management and prioritize scarce resources among the incidents. Due to the scope of incidents involving Area Commands and the likelihood of cross-jurisdictional operations, Area Commands are frequently established as Unified Area Commands, working under the same principles as a Unified Command.

Authority Having Jurisdiction: The Authority Having Jurisdiction (AHJ) is an entity that can create and administer processes to qualify, certify, and credential personnel for incident-related positions. AHJs include state, tribal, or Federal government departments and agencies, training commissions, NGOs, or companies, as well as local organizations such as police, fire, public health, or public works departments.

Emergency Operations Center: An EOC is a facility from which staff provide information management, resource allocation and tracking, and/or advanced planning support to personnel on scene or at other EOCs (e.g., a state center supporting a local center).

Incident Commander: The Incident Commander is the individual responsible for on-scene incident activities, including developing incident objectives and ordering and releasing resources. The Incident Commander has overall authority and responsibility for conducting incident operations.

Multiagency Coordination Group: MAC Groups, sometimes called policy groups, typically consist of agency administrators or executives from organizations or their designees. MAC Groups provide policy guidance to incident personnel, support resource prioritization and allocation, and enable decision making among elected and appointed officials and senior executives in other organizations as well as those directly responsible for incident management.

Unified Command: When more than one agency has incident jurisdiction, or when incidents cross political jurisdictions, the use of Unified Command enables multiple organizations to

perform the functions of the Incident Commander jointly. Each participating partner maintains authority, responsibility, and accountability for its personnel and other resources while jointly managing and directing incident activities through the establishment of a common set of incident objectives, strategies, and a single Incident Action Plan (IAP).

F. Supersession

This document supersedes the NIMS document issued in December 2008 and NIMS Guides 0001 and 0002 (both issued March 2006).

II. Resource Management

NIMS resource management guidance enables many organizational elements to collaborate and coordinate to systematically manage resources—personnel, teams, facilities, equipment, and supplies. Most jurisdictions or organizations do not own and maintain all the resources necessary to address all potential threats and hazards. Therefore, effective resource management includes leveraging each jurisdiction's resources, engaging private sector resources, involving volunteer organizations, and encouraging further development of mutual aid agreements.

This component includes three sections: Resource Management Preparedness, Resource Management During an Incident, and Mutual Aid.

A. Resource Management Preparedness

Resource management preparedness involves: identifying and typing resources; qualifying, certifying, and credentialing personnel; planning for resources; and acquiring, storing, and inventorying resources.

Identifying and Typing Resources

Resource typing is defining and categorizing incident resources by capability. Resource typing definitions establish a common language for discussing resources by defining minimum capabilities for personnel, teams, facilities, equipment, and supplies. Resource typing enables communities to plan for, request, and have confidence that the resources they receive have the capabilities they requested.

FEMA leads the development and maintenance of resource typing definitions for resources shared on a local, interstate, regional, or national scale. Jurisdictions can use these definitions to categorize local assets. When identifying which resources to type at the national level, FEMA selects resources that:

- Are widely used and sharable;
- Can be shared and/or deployed across jurisdictional boundaries through mutual aid agreements or compacts;
- Can be identified by the following characteristics:
  - ***Capability***: The core capability[6] for which the resource is most useful;
  - ***Category***: The function for which a resource would be most useful (e.g., firefighting, law enforcement, health and medical);
  - ***Kind***: A broad characterization, such as personnel, teams, facilities, equipment and supplies; and

[6] Core capabilities, as defined in the National Preparedness Goal, are essential elements for the execution of the five mission areas: Prevention, Protection, Mitigation, Response, and Recovery.

  - ***Type***: A resource's level of minimum capability to perform its function;
    - The specific metrics used for determining a resource's type depend on the kind of resource and the mission envisioned (e.g., a mobile kitchen unit is typed according to the number of meals it can produce, while dump trucks are typed according to haul capacity);
    - Type 1 is a higher capability than Type 2, which is higher capability than Type 3, etc.;
    - The level of capability is based on size, power, and capacity (for equipment) or experience and qualifications (for personnel or teams);
- Can be identified, inventoried, and tracked to determine availability;
- Are used for incident management, support, and/or coordination under ICS and/or in EOCs; and
- Are sufficiently interoperable or compatible to allow for deployment through common systems for resource ordering, managing, and tracking.

Resource users at all levels apply these standards to identify and inventory resources. Resource kind subcategories define the capabilities more precisely.

Resource Typing Library Tool

The Resource Typing Library Tool (RTLT) is an online catalog of NIMS resource typing definitions and job titles/position qualifications. The RTLT is accessible at http://www.fema.gov/resource-management-mutual-aid. From the RTLT home page, users can search by resource type, discipline, core capability, or other key words.

Qualifying, Certifying, and Credentialing Personnel

Qualifying, certifying, and credentialing are the essential steps, led by an AHJ, that help ensure that personnel deploying through mutual aid agreements have the knowledge, experience, training, and capability to perform the duties of their assigned roles. These steps help to ensure that personnel across the Nation are prepared to perform their incident responsibilities based on criteria that are standard nationwide.

Qualification is the process through which personnel meet the minimum established criteria—training, experience, physical and medical fitness, and capability—to fill specific positions.

Certification/Recertification is the recognition from the AHJ or a third party[7] stating that an individual has met and continues to meet established criteria and is qualified for a specific position.

Credentialing occurs when an AHJ or third party provides documentation—typically an identification card or badge—that identifies personnel and authenticates and verifies their qualification for a particular position. While credentialing includes issuing credentials such as

[7] Certain positions require third-party certification and/or credentialing from an accredited body such as a state licensure board for medical professionals.

identification cards, it is separate from an incident-specific badging process, which includes identity verification, qualification, and deployment authorization.

Applying the Qualification, Certification, and Credentialing Process

The NIMS qualification, certification, and credentialing process (see Figure 1) uses a performance-based approach. This process enables communities to plan for, request, and have confidence in personnel assigned from other organizations through mutual aid agreements.

Nationally standardized criteria and minimum qualifications for positions provide a consistent baseline for qualifying and credentialing the incident workforce. Along with the job title and position qualifications, the position task book (PTB) is a basic tool that underpins the NIMS performance-based qualification process. PTBs describe the minimum competencies, behaviors, and tasks necessary to be qualified for a position. PTBs provide the basis for a qualification, certification, and credentialing process that is standard nationwide.

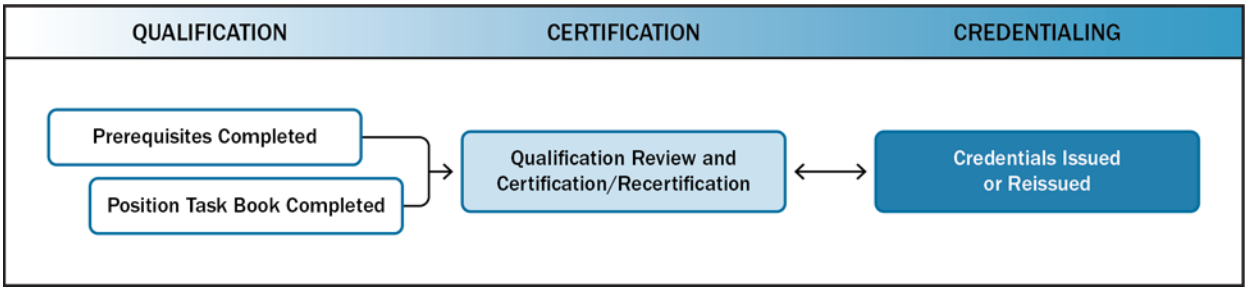


Figure 1: Qualification, Certification, and Credentialing of Incident Personnel

FEMA recommends minimum qualifications, but it is AHJs across the Nation that establish, communicate, and administer the qualification and credentialing process for individuals seeking qualification for positions under that AHJ's purview. AHJs have the authority and responsibility to develop, implement, maintain, and oversee the qualification, certification, and credentialing process within their organization or jurisdiction. AHJs may impose additional requirements outside of NIMS for local needs. In some cases, the AHJ may support multiple disciplines that collaborate as a part of a team (e.g., an Incident Management Team [IMT]).

Planning for Resources

Jurisdictions and organizations work together before incidents occur to develop plans for identifying, managing, estimating, allocating, ordering, deploying, and demobilizing resources. The planning process includes identifying resource requirements based on the threats to, and vulnerabilities of, the jurisdiction or organization. Planning also includes developing alternative strategies to obtain needed resources. Resource management personnel should consider resources necessary to support all mission areas (Prevention, Protection, Mitigation, Response, and Recovery).[8] Resource management strategies that planners should consider include:

- Stockpiling resources;

[8] The National Preparedness Goal and the five National Planning Frameworks describe the mission areas in greater detail.

- Establishing mutual aid agreements to obtain resources from neighboring jurisdictions;
- Determining how and where to reassign existing resources from non-essential tasks; and/or
- Developing contracts to acquire resources from vendors rapidly when needed.

Resource planners consider the urgency of needs, whether sufficient quantities of items are on hand, and whether the items can be produced quickly enough to meet demand. Stockpiling presents issues concerning shelf life and durability; however, the alternative of acquiring resources just in time also has potential pitfalls. Planners should verify, for example, that multiple jurisdictions are not relying on the same assets or vendors (such as hospitals in the same city relying on one supplier's stock of surge medical supplies that may be adequate for only one hospital). Jurisdictions should also incorporate protocols for handling and distributing donated resources.

Capability Estimation

Estimating resource needs is key to resource planning. Through capability estimation, jurisdictions assess their ability to take a course of action. The resulting capability estimate feeds into the resource section of the plan or annex. Capability estimation helps answer the following questions:

- What do we need to prepare for?
- What resources do we have that allow us to achieve our targets?
- What resources can we obtain through mutual aid to be prepared to meet our targets?

The outputs of this process inform a variety of preparedness efforts, including strategic, operational, and/or tactical planning; development of mutual aid agreements and compacts; and hazard mitigation planning.

For activities that need surge capacity, planning often includes pre-positioning resources. Plans should anticipate conditions or circumstances that trigger a reaction, such as restocking supplies when inventories reach a predetermined minimum.

Acquiring, Storing, and Inventorying Resources

Organizations acquire, store, and inventory resources for day-to-day operations, as well as additional resources that the organization has stockpiled for incidents. Those with resource management responsibilities should plan for periodic replenishments, preventive maintenance, and capital improvements. They should also plan for any ancillary support, supplies, or space that may be needed for large or complex resources. Effective resource management involves establishing a resource inventory and maintaining the currency and accuracy of the information. While a resource inventory can be as simple as a paper spreadsheet, many resource managers use information technology (IT)-based inventory systems to track the status of resources and maintain an accurate list of available resources. Accurate resource inventories not only enable organizations to resource incidents promptly, but also to support day-to-day resource management activities such as reconciliation, accounting, and auditing.

Resource Inventorying vs. Resource Tracking

For NIMS purposes, resource inventorying refers to the preparedness activity done outside of incident response. Inventories include an up-to-date count and pertinent details about an organization's resources. Inventories often provide the basis for resource tracking during an incident.

Resource tracking occurs during an incident and includes the number and status of resources assigned to an incident, the organizational element to which they are assigned, and their progress against applicable work/rest ratios. Incident needs drive the numbers and types of resources tracked.

An effective resource inventory includes the following information regarding each resource:

- ***Name***: The resource's unique name.
- ***Aliases***: Any other names for the resource, whether formal or informal. These can be radio call signs, license numbers, nicknames, or anything else that helps users identify the resource.
- ***Status***: The resource's current condition or readiness state.
- ***Resource Typing Definition or Job Title***: This can be either a standard NIMS resource typing definition or job title/position qualification or—for non-typed resources—a local, state, or tribal definition.
- ***Mutual Aid Readiness***: The status of whether the resource is available and ready for deployment under mutual aid.
- ***Home Location***: The resource's permanent storage location, base, or office. This should also include the home location's associated latitude/longitude and United States National Grid coordinates to ensure interoperability with mapping and decision support tools.
- ***Present Location***: The resource's current storage location, base, office, or deployment assignment with associated latitude/longitude and United States National Grid coordinates.
- ***Point of Contact***: Individuals able to provide information and communicate essential information related to the resource.
- ***Owner***: The agency, company, person, or other entity that owns the resource.
- ***Manufacturer/Model (Equipment Only)***: The entity that built the resource and the resource's model name/number. This section also includes the serial number—the resource's unique identifying number. This is a real-world inventory control number or other value used in official records.
- ***Contracts***: Purchase, lease, rental, or maintenance agreements or other financial agreements associated with the resource.
- ***Certifications***: Documentation that validates the official qualifications, certifications, or licenses associated with the resource.
- ***Deployment Information***: Information needed to request a resource includes:

- ***Minimum Lead Time (in hours)***: The minimum amount of time a resource needs to prepare for deployment to the incident.
- ***Maximum Deployment Time (in days)***: The maximum amount of time a resource can be deployed or involved before it needs to be pulled back for maintenance, recovery, or resupply.
- ***Restrictions***: Any restrictions placed on the resource use, deployable area, capabilities, etc.
- ***Reimbursement Process***: Any information regarding repayment for items that are reimbursable.
- ***Release and Return Instructions***: Any information regarding the release and return of the resource.
- ***Sustainability Needs***: Any information regarding actions necessary to maintain the usability of the resource.
- ***Custom Attributes***: A customizable field that an agency can add to resource records. This can contain any necessary information that standard fields do not contain.

Resource inventories also account for (and mitigate) the potential for double-counting personnel and/or equipment. Resource summaries should clearly reflect any overlap of personnel, supplies, and/or equipment across different resource pools to avoid overstating the total resources.

B. Resource Management During an Incident

The resource management process during an incident includes standard methods to identify, order, mobilize, and track resources. In some cases, the identification and ordering process is compressed, such as when an Incident Commander identifies the specific resources necessary for a given task and orders those resources directly. However, in larger, more complex incidents, the Incident Commander relies on the resource management process and personnel in the ICS and EOC organizations to identify and meet resource needs. Figure 2 depicts the six primary tasks of resource management during an incident.

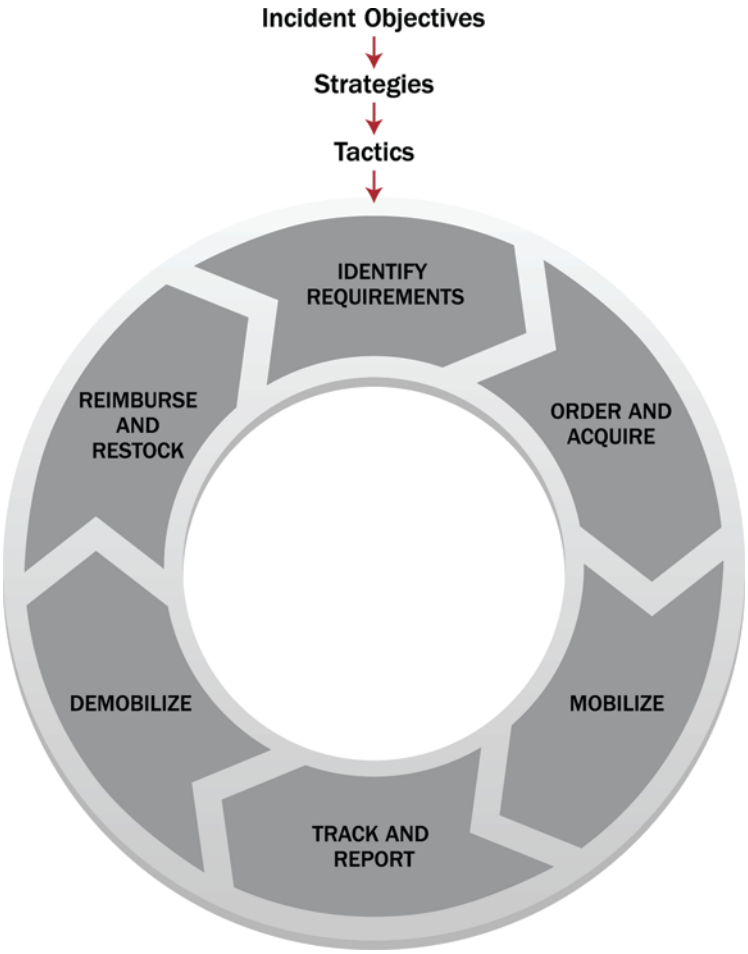


Figure 2: Resource Management Process

Identifying Requirements

During an incident, personnel continually identify, validate, and refine resource needs. This process involves identifying the type and quantity of resources needed, the location where resources should be sent, and who will receive and use the resources.

Resource availability and needs constantly change as an incident evolves. Consequently, incident management personnel and their affiliated organizations should coordinate as closely and as early as possible, both in advance of and during incidents.

Ordering and Acquiring

Both incident and EOC staff make initial and ongoing assessments of resource requirements and either activate or request those resources. Incident personnel can order additional resources by executing contracts, implementing mutual aid agreements, or requesting assistance from another level of government (e.g., a local government to a state, or a state to the Federal Government).

Incident and/or EOC personnel request resources based on incident priorities and objectives. They base decisions about resource allocation on jurisdictional or organization protocol (e.g., minimum staffing levels) and, when applicable, the resource demands of other incidents. The organization providing resources consents to the request and communicates any discrepancies between requested resources and those available for delivery.

Resource Requests

Organizations that request resources should provide enough detail to ensure that those receiving the request understand what is needed. Using NIMS resource names and types helps ensure that requests are clearly communicated and understood. Requesting organizations should include the following information in the request:

- Detailed item description including quantity, kind, and type, if known, or a description of required capability and/or intended use if not;
  - If suitable substitute resources or preferred sources exist, these should also be indicated;
  - If the resource is not a common or standard incident resource, then the requestor should provide detailed specifications;
- Required arrival date and time;
- Required delivery or reporting location;
- The position title of the individual to whom the resource should report; and
- Any incident-specific health or safety concerns (e.g., vaccinations, adverse living/working conditions, or identified environmental hazards).

Personnel are assigned based on their qualifications and the needs of the incident, as well as any jurisdictional licensing requirements or limitations (i.e., personnel in some fields, including law enforcement and medicine, have limited authority outside of the jurisdiction in which they are sworn or licensed).

Incident Assignments

Effective and safe incident management depends on all personnel executing their responsibilities according to established guidelines. Personnel deploy to incidents at the request of the appropriate authority. Individuals remain deployment-ready by maintaining the skills, knowledge, certifications, physical fitness, and other items, such as equipment, that their organization requires or recommends.

Upon notification of deployment, individuals should:

- Review the most recent situation report (if available);
- Identify assignment, deployment location, and travel arrangements;
- Identify assigned supervisor and associated contact information, if possible;
- Obtain a copy of assignment paperwork;
- Review any briefings on worksite security or access procedures and any special environmental or health concerns for the deployment area (if available); and
- Ensure/verify coverage for day-to-day job responsibilities.

When personnel reach their designated incident worksite, they should adhere to accountability procedures, including:

- ***Check-In***: Report in to receive an assignment. (Applies to all personnel regardless of agency affiliation)
- ***Recordkeeping***: Follow incident procedures for documenting their activities. Maintaining complete and accurate records helps with state and Federal assistance, reimbursements, and potential future litigation.
- ***Communication***: Observe radio and/or telephone procedures; use plain language and clear text, not codes.
- ***Checkout***: When notified of their demobilization, follow the local checkout procedures before leaving the incident area. Personnel should complete all work in progress (unless otherwise directed); ensure all records and files are up to date; return or transfer any equipment received in support of the incident; and brief incoming personnel, if applicable, on work status and assignments.

Unrequested Resources

During incidents, responders sometimes come to an incident area without being requested. Such personnel converging on a site, commonly referred to as self-dispatching or self-deploying, may interfere with incident management and place an extra logistical and management burden on an already stressed system by:

- Creating additional supervisory, logistical, and safety needs;
- Depleting the resources needed to provide continued services to their home community;
- Complicating resource tracking and accountability; and/or
- Interfering with the access of formally requested resources.

Responders should wait for official deployment notification rather than self-deploying to an incident.

Mobilizing

Personnel and other resources begin mobilizing when notified by the requesting jurisdiction or by an intermediary acting on its behalf, such as the state Emergency Management Assistance Compact (EMAC) coordinator. At the time of notification, deploying personnel should be notified regarding:

- The date, time, and place of departure;
- Mode of transportation to the incident;
- Estimated date and time of arrival;
- Reporting location (address, position title, and phone number or radio frequency);
- Anticipated incident assignment;
- Anticipated duration of deployment;
- Resource order number;
- Incident number; and
- Applicable cost and funding codes.

Resource tracking directly links to the mobilization process. Resources arriving on scene check in according to the receiving organization's check-in process.

The mobilization process includes:

- Conducting incident-specific deployment planning;
- Equipping;
- Providing just-in-time training;
- Designating assembly points; and
- Delivering resources to the incident on schedule and in line with priorities and budgets.

Mobilizing fixed facility resources, such as laboratories, hospitals, EOCs, shelters, and waste management systems, involves activation rather than deployment. Plans and systems to monitor resource mobilization status should be flexible enough to adapt to both types of resources. Managers plan and prepare for the demobilization process at the same time they begin mobilizing resources.

Survivors as Resources

Before emergency responders can mobilize and arrive, neighbors and bystanders are often the first people to provide life-saving assistance. The natural desire to help does not disappear once responders arrive on the scene. Incident management personnel should anticipate this and have plans to use these volunteers' capabilities safely and effectively.

Private and Voluntary Organizations

Voluntary organizations, such as the American Red Cross or Medical Reserve Corps, also mobilize and provide valuable assistance before, during, and after incidents. These groups provide a structure to integrate volunteers into incident activities. They also frequently have established relationships with the community, provide assistance that governmental organizations cannot, and support requests through formal resource-ordering processes.

Tracking and Reporting

Incident managers use established procedures to track resources from mobilization through demobilization. Resource tracking occurs prior to, during, and after an incident. This process helps staff prepare to receive and use resources; tracks resource location; facilitates the safety and security of personnel, equipment, teams, and facilities; and enables effective resource coordination and movement.

Information Management Systems for Resource Management

Information management systems enhance resource status information flow by providing real-time data to jurisdictions, incident personnel, and their affiliated organizations. Information management systems used to support resource management include location-enabled situational awareness and decision support tools with resource tracking that links to the entity's resource inventory(s).

Demobilizing

The goal of demobilization is the orderly, safe, and efficient return of a resource to its original location and status. Once resources are no longer needed on an incident, those responsible for resources should demobilize them. The resource requestor and provider may agree to reassign a resource rather than demobilize it. Prior to demobilization, incident staff responsible for the planning and logistics functions collaborate to plan how resources are rehabilitated, replenished, disposed of, and/or returned or restored to operational condition.

Reimbursing and Restocking

Reimbursement includes the payment of expenses incurred by resource providers for specific activities. Reimbursement processes are important for establishing and maintaining resource readiness and establishing the means to pay providers in a timely manner. Processes include mechanisms for collecting bills, validating costs against the scope of the work, replacing or repairing damaged equipment, and accessing reimbursement programs. Reimbursement procedures are often specified in mutual aid and assistance agreements.

C. Mutual Aid

Mutual aid involves sharing resources and services between jurisdictions or organizations. Mutual aid occurs routinely to meet the resource needs identified by the requesting organization. This assistance can include the daily dispatch of law enforcement, emergency medical services (EMS), and fire service resources between local communities, as well as the movement of resources within a state or across state lines when larger-scale incidents occur. Mutual aid can provide essential assistance to fill mission needs. NIMS resource management guidance supports mutual aid efforts nationwide.

Mutual Aid Agreements and Compacts

Mutual aid agreements establish the legal basis for two or more entities to share resources. Mutual aid agreements exist in various forms among and between all levels of government. These agreements support effective and efficient resource management. Mutual aid agreements may authorize mutual aid between two or more neighboring communities, among all jurisdictions within a state, between states, between Federal agencies, and/or internationally. Mutual aid also exists through formal and informal arrangements developed by tribal governments, NGOs, and in various forms within the private sector.

Emergency Management Assistance Compact

EMAC is a congressionally ratified mutual aid compact that defines a non-Federal, state-to-state system for sharing resources across state lines during an emergency or disaster. Signatories include all 50 states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands. EMAC's unique relationships with states, regions, territories, and Federal organizations, such as FEMA and the National Guard Bureau, enable it to move a wide variety of resources to meet the jurisdictions' needs.

These mutual aid agreements often address participating entities' liability, compensation, and procedures, and might include some of the following topics:

- ***Reimbursement***: Mutual aid services are either paid or unpaid (e.g., based on providing reciprocal services). Some mutual aid agreements specify reimbursement parameters.
- ***Recognition of Licensure and Certification***: Guidelines to ensure recognition of licensures across geopolitical boundaries.
- ***Procedures for Mobilization (Request, Dispatch, and Response)***: Specific procedures for parties to request and dispatch resources through mutual aid.
- ***Protocols for Voice and Data Interoperability***: Protocols that specify how different communications and IT systems share information.
- ***Protocols for Resource Management***: Standard templates for packaging resources based on NIMS resource typing definitions and/or local inventory systems.

Mutual Aid Process

Upon receipt of a request for mutual aid, the providing jurisdiction evaluates the request against its capacity to accommodate the temporary loss of the resource(s). For example, resource

managers in a fire department consider whether the department could still meet its community's needs after deploying requested equipment and personnel to another jurisdiction.

If the providing jurisdiction determines it can accommodate the requested deployment of resources, it identifies specific resources and arranges their deployment in accordance with the terms of the mutual aid agreement. The receiving jurisdiction can decline resources if they do not meet its needs.

III. Command and Coordination

Local authorities handle most incidents using the communications systems, dispatch centers, and incident personnel within a single jurisdiction. Larger and more complex incidents, however, may begin with a single jurisdiction, but rapidly expand to multijurisdictional and/or multidisciplinary efforts necessitating outside resources and support. Standard incident command and coordination systems allow the efficient integration of these outside resources and enable assisting personnel from anywhere in the Nation to participate in the incident management structure. The Command and Coordination component of NIMS describes the systems, principles, and structures that provide a standard, national framework for incident management.

Regardless of the size, complexity, or scope of the incident, effective command and coordination—using flexible and standard processes and systems—helps save lives and stabilize the situation. Incident command and coordination consist of four areas of responsibility:

1. Tactical activities to apply resources on scene;
2. Incident support, typically conducted at EOCs,[9] through operational and strategic coordination, resource acquisition and information gathering, analysis, and sharing;
3. Policy guidance and senior-level decision making; and
4. Outreach and communication with the media and public to keep them informed about the incident.

MACS exist to coordinate these four areas across the different NIMS functional groups: ICS, EOCs, MAC Groups, and Joint Information Systems (JIS). The Command and Coordination component describes these MACS structures and explains how various elements operating at different levels of incident management interface with one another. By describing unified doctrine with common terminology, organizational structures, and operational protocols, NIMS enables all those involved in an incident—from the Incident Commander at the scene to national leaders in a major disaster—to harmonize and maximize the effects of their efforts.

[9] Because incident support is conducted in a wide variety of different facilities, as well as virtual structures, NIMS uses the term “EOC” to refer to all such facilities, including emergency coordination centers.

A. NIMS Management Characteristics

The following characteristics are the foundation of incident command and coordination under NIMS and contribute to the strength and efficiency of the overall system:

- Common Terminology
- Management by Objectives
- Manageable Span of Control
- Comprehensive Resource Management
- Establishment and Transfer of Command
- Chain of Command and Unity of Command[10]
- Dispatch/Deployment
- Modular Organization
- Incident Action Planning
- Incident Facilities and Locations
- Integrated Communications
- Unified Command
- Accountability
- Information and Intelligence Management

Common Terminology

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

- ***Organizational Functions***: Major functions and functional units with incident responsibilities are named and defined. Terminology for incident organizational elements is standard and consistent.
- ***Resource Descriptions***: Major resources—including personnel, equipment, teams, and facilities—are given common names and are typed to help avoid confusion and to enhance interoperability.
- ***Incident Facilities***: Incident management facilities are designated using common terminology.

Modular Organization

ICS and EOC organizational structures develop in a modular fashion based on an incident's size, complexity, and hazard environment. Responsibility for establishing and expanding ICS organizations and EOC teams ultimately rests with the Incident Commander (or Unified Command) and EOC director.[11] Responsibility for functions that subordinates perform defaults to the next higher supervisory position until the supervisor delegates those responsibilities. As

[10] The concepts of "command" and "unity of command" have distinct legal meanings for military forces and operations. For military forces, command runs from the President to the Secretary of Defense to the commander of the combatant command to the commander of the forces.

[11] The term "EOC director" is used throughout NIMS to refer to the individual who heads the team that works in an EOC when it is activated. In actual practice, this position may have a variety of titles, such as EOC Manager or EOC Coordinator, depending on the plans and procedures of the jurisdiction/organization.

incident complexity increases, organizations expand as the Incident Commander, Unified Command, EOC director, and subordinate supervisors delegate additional functional responsibilities.

Management by Objectives

The Incident Commander or Unified Command[12] establishes objectives that drive incident operations. Management by objectives includes the following:

- Establishing specific, measurable objectives;
- Identifying strategies, tactics, tasks, and activities to achieve the objectives;
- Developing and issuing assignments, plans, procedures, and protocols for various incident management functional elements to accomplish the identified tasks; and
- Documenting results against the objectives to measure performance, facilitate corrective actions, and inform development of incident objectives for the subsequent operational period.

Incident Action Planning

Coordinated incident action planning guides incident management activities. IAPs represent concise, coherent means of capturing and communicating incident objectives, tactics, and assignments for operational and support activities.

Every incident should have an action plan; however, not all incidents need written plans. The necessity for written plans depends on incident complexity, command decisions, and legal requirements. Formal IAPs are not always developed for the initial operational period of no-notice incidents. However, if an incident is likely to extend beyond one operational period, becomes more complex, or involves multiple jurisdictions and/or agencies, preparing a written IAP becomes increasingly important to maintain unity of effort and effective, efficient, and safe operations.

Staff in EOCs also typically conduct iterative planning and produce plans to guide their activities during specified periods, though these are typically more strategic than IAPs.

Manageable Span of Control

Maintaining an appropriate span of control helps ensure an effective and efficient incident management operation. It enables management to direct and supervise subordinates and to communicate with and manage all resources under their control. The type of incident, nature of the task, hazards and safety factors, experience of the supervisor and subordinates, and communication access between the subordinates and the supervisor are all factors that influence manageable span of control.

[12] When an Area Command is established, many of the responsibilities of an Incident Commander or Unified Command also apply to an Area Commander or Unified Area Command. Area Command is discussed in more detail in Section III.B under Area Command or in the ICS Tab 7—Consolidating the Management of Multiple Incidents.

Manageable Span of Control

The optimal span of control for incident management is one supervisor to five subordinates; however, effective incident management frequently necessitates ratios significantly different from this. The 1:5 ratio is a guideline, and incident personnel use their best judgment to determine the actual distribution of subordinates to supervisors for a given incident or EOC activation.

Incident Facilities and Locations

Depending on the incident size and complexity, the Incident Commander, Unified Command, and/or EOC director establish support facilities for a variety of purposes and direct their identification and location based on the incident. Typical facilities include the Incident Command Post (ICP), incident base, staging areas, camps, mass casualty triage areas, points-of-distribution, and emergency shelters.

Comprehensive Resource Management

Resources include personnel, equipment, teams, supplies, and facilities available or potentially available for assignment or allocation. Maintaining an accurate and up-to-date inventory of resources is an essential component of incident management. Section II, the Resource Management component of this document, describes this in more detail.

Integrated Communications

Leadership at the incident level and in EOCs facilitates communication through the development and use of a common communications plan, interoperable communications processes, and systems that include voice and data links. Integrated communications provide and maintain contact among and between incident resources, enable connectivity between various levels of government, achieve situational awareness, and facilitate information sharing. Planning, both in advance of and during an incident, addresses equipment, systems, and protocols necessary to achieve integrated voice and data communications. Section IV, the Communications and Information Management component of this document, describes this in more detail.

Establishment and Transfer of Command

The Incident Commander or Unified Command should clearly establish the command function at the beginning of an incident. The jurisdiction or organization with primary responsibility for the incident designates the individual at the scene responsible for establishing command and protocol for transferring command. When command transfers, the transfer process includes a briefing that captures essential information for continuing safe and effective operations, and notifying all personnel involved in the incident.

Unified Command

When no one jurisdiction, agency or organization has primary authority and/or the resources to manage an incident on its own, Unified Command may be established. In Unified Command, there is no one “commander.” Instead, the Unified Command manages the incident by jointly approved objectives. A Unified Command allows these participating organizations to set aside issues such as overlapping and competing authorities, jurisdictional boundaries, and resource ownership to focus on setting clear priorities and objectives for the incident. The resulting unity

of effort allows the Unified Command to allocate resources regardless of ownership or location. Unified Command does not affect individual agency authority, responsibility, or accountability.

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 each individual only reports to one person. This clarifies reporting relationships and reduces confusion caused by multiple, conflicting directives, enabling leadership at all levels to effectively direct the personnel under their supervision.

Accountability

Effective accountability for resources during an incident is essential. Incident personnel should adhere to principles of accountability, including check-in/check-out, incident action planning, unity of command, personal responsibility, span of control, and resource tracking.

Dispatch/Deployment

Resources should deploy only when appropriate authorities request and dispatch them through established resource management systems. Resources that authorities do not request should refrain from spontaneous deployment to avoid overburdening the recipient and compounding accountability challenges.

Information and Intelligence Management

The incident management organization establishes a process for gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.[13] Information and intelligence management includes identifying essential elements of information (EEI) to ensure personnel gather the most accurate and appropriate data, translate it into useful information, and communicate it with appropriate personnel. Section IV, the Communications and Information Management component of this document, describes this in more detail.

[13] In NIMS, "intelligence" refers exclusively to threat-related information developed by law enforcement, medical surveillance, and other investigative organizations.

B. Incident Command System (ICS)

ICS is a standardized approach to the command, control, and coordination of on-scene incident management that provides a common hierarchy within which personnel from multiple organizations can be effective. ICS specifies an organizational structure for incident management that integrates and coordinates a combination of procedures, personnel, equipment, facilities, and communications. Using ICS for every incident helps hone and maintain skills needed to coordinate efforts effectively. ICS is used by all levels of government as well as by many NGOs and private sector organizations. ICS applies across disciplines and enables incident managers from different organizations to work together seamlessly. This system includes five major functional areas, staffed as needed,[14] for a given incident: Command, Operations, Planning, Logistics, and Finance/Administration.

Incident Command and Unified Command

Incident command is responsible for the overall management of the incident. A single Incident Commander or Unified Command conducts the command function on an incident. Command and General Staff support the incident command to meet the incident's needs.

Single Incident Commander

When an incident occurs within a single jurisdiction and without jurisdictional or functional agency overlap, the appropriate authority designates a single Incident Commander who has overall incident management responsibility. In some cases where incident management crosses jurisdictional and/or functional agency boundaries, the various jurisdictions and organizations may still agree to designate a single Incident Commander. Figure 3 depicts an example organizational structure for an ICS organization with a single Incident Commander.

[14] ICS and EOC staff make many decisions based on unique criteria, including the incident situation, supervisor preferences, resource availability, and applicable laws, policies, or standard operating procedures (SOP). The document uses the phrase "as needed" to acknowledge this flexibility.

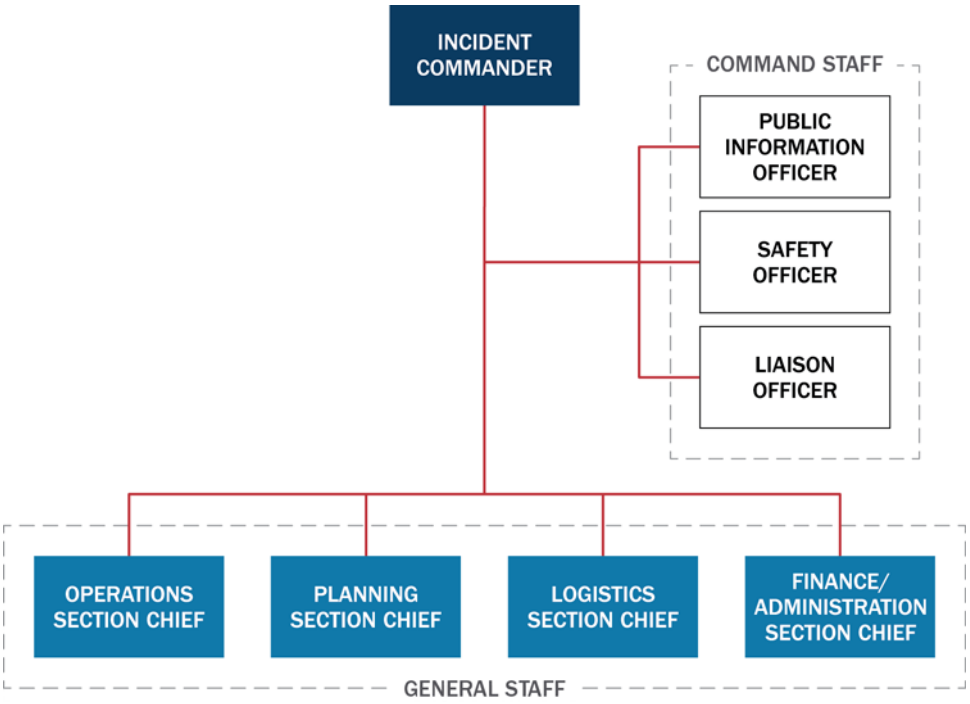


Figure 3: Example of an ICS Organization with a Single Incident Commander

Unified Command

Unified Command improves unity of effort in multijurisdictional or multiagency incident management. The use of Unified Command enables jurisdictions and those with authority or functional responsibility for the incident to jointly manage and direct incident activities through the establishment of a common set of incident objectives, strategies, and a single IAP. However, each participating partner maintains authority, responsibility, and accountability for its personnel and other resources, and each member of Unified Command is responsible for keeping other members of Unified Command informed.

Responsibilities of the Incident Commander and Unified Command

Whether using a single Incident Commander or a Unified Command, the command function:

- Establishes a single ICP for the incident;
- Establishes consolidated incident objectives, priorities, and strategic guidance, and updating them every operational period;
- Selects a single section chief for each position on the General Staff needed based on current incident priorities;
- Establishes a single system for ordering resources;
- Approves a consolidated IAP for each operational period;
- Establishes procedures for joint decision making and documentation; and
- Captures lessons learned and best practices.

Unified Command Composition

The exact composition of the Unified Command depends on factors such as incident location (i.e., which jurisdictions or organizations are involved) and the nature of the incident (i.e., which agencies from the jurisdiction(s) or organization(s) involved are needed). Figure 4 depicts a sample Unified Command structure. The organizations participating in the Unified Command use a collaborative process to establish and rank incident priorities and determine incident objectives.

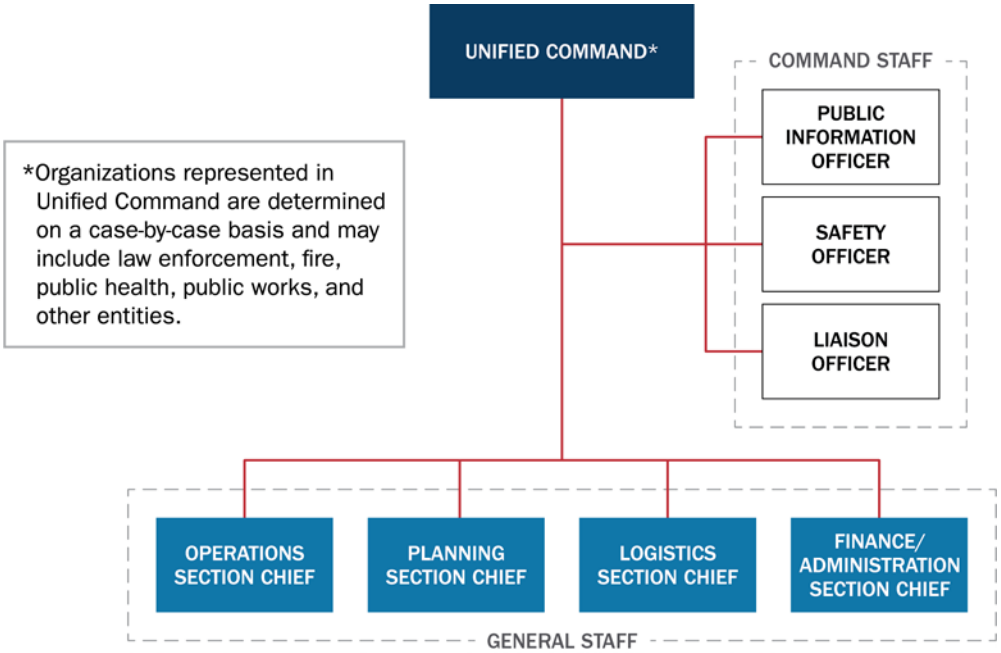


Figure 4: Example of an ICS Organization with Unified Command

Single Incident Commander and Unified Command

Single Incident Commander: The Incident Commander is solely responsible (within the limits of his or her authority) for establishing incident objectives and is responsible for ensuring that incident activities work to accomplish objectives.

Unified Command: The individuals designated by their jurisdictional or organizational authorities (or by departments within a single jurisdiction) jointly determine priorities and objectives, allocate resources, and work together to ensure the execution of integrated incident operations and maximize the use of assigned resources.

Agencies or organizations involved in the incident that lack jurisdictional responsibility or authorities are referred to as cooperating and/or assisting agencies. Whether represented in Unified Command or through the Liaison Officer, every jurisdiction, organization, and/or agency representative is responsible for communicating agency-specific information, including:

- Statutory authorities and responsibilities;
- Resource availability and capabilities;
- Constraints, limitations, concerns; and
- Areas of agreement and disagreement between agency officials.

Command Staff

The Incident Commander or Unified Command assigns Command Staff as needed to support the command function. The Command Staff typically includes a Public Information Officer (PIO), a Safety Officer, and a Liaison Officer who report directly to the Incident Commander or Unified Command and have assistants as necessary. The Incident Commander or Unified Command may appoint additional advisors as needed.

Public Information Officer

The PIO interfaces with the public, media, and/or with other agencies with incident-related information needs. The PIO gathers, verifies, coordinates, and disseminates accessible,[15] meaningful, and timely information on the incident for both internal and external audiences. The PIO also monitors the media and other sources of public information to collect relevant information and transmits this information to the appropriate components of the incident management organization. In incidents that involve PIOs from different agencies, the Incident Commander or Unified Command designates one as the lead PIO. All PIOs should work in a unified manner, speaking with one voice, and ensure that all messaging is consistent. The Incident Commander or Unified Command approves the release of incident-related information. In large-scale incidents, the PIO participates in or leads the Joint Information Center (JIC).

Safety Officer

The Safety Officer monitors incident operations and advises the Incident Commander or Unified Command on matters relating to the health and safety of incident personnel. Ultimate responsibility for the safe conduct of incident management rests with the Incident Commander or Unified Command and supervisors at all levels. The Safety Officer is responsible to the Incident Commander or Unified Command for establishing the systems and procedures necessary to assess, communicate, and mitigate hazardous environments. This includes developing and maintaining the incident Safety Plan, coordinating multiagency safety efforts, and implementing measures to promote the safety of incident personnel and incident sites. The Safety Officer stops and/or prevents unsafe acts during the incident. Agencies, organizations, or jurisdictions that contribute to joint safety management efforts do not lose their individual responsibilities or authorities for their own programs, policies, and personnel. Rather, each contributes to the overall effort to protect all personnel involved in the incident.

Liaison Officer

The Liaison Officer is the incident command's point of contact for representatives of governmental agencies, jurisdictions, NGOs, and private sector organizations that are not included in the Unified Command. Through the Liaison Officer, these representatives provide input on their agency, organization, or jurisdiction's policies, resource availability, and other incident-related matters. Under either a single Incident Commander or a Unified Command structure, representatives from assisting or cooperating jurisdictions and organizations coordinate through the Liaison Officer. The Liaison Officer may have assistants.

[15] Accessible to all individuals, including those with limited English proficiency and individuals with disabilities, so that access to and use of any such information and data is comparable to the access to and use of the information and data by members of the public who are not individuals with disabilities.

Additional Command Staff Positions

Additional Command Staff positions may be necessary, depending on the incident and specific requirements established by incident command. The Incident Commander or Unified Command may appoint technical specialists to serve as command advisors. Command Staff advisors are distinguished from officers because they serve in advisory capacities and lack the authority to direct incident activities.

General Staff

The General Staff consists of the Operations, Planning, Logistics, and Finance/Administration Section Chiefs. These individuals are responsible for the functional aspects of the incident command structure. The Incident Commander or Unified Command activates these section chiefs as needed. These functions default to the Incident Commander or Unified Command until a section chief is assigned. The section chiefs may have one or more deputies as necessary. The sections are discussed more fully below.

Operations Section

The Incident Commander or Unified Command selects the Operations Section Chief based on current incident priorities and should review that selection periodically as the incident evolves. Operations Section personnel plan and perform tactical activities to achieve the incident objectives established by the Incident Commander or Unified Command. Objectives typically focus on saving lives, reducing the immediate hazard, protecting property and the environment, establishing situational control, and restoring normal operations.

Incident operations can be organized and executed in many ways. The Operations Section Chief organizes the section based on the nature and scope of the incident, the jurisdictions and organizations involved, and the incident's priorities, objectives, and strategies. Key functions of Operations Section personnel include the following:

- Directing the management of tactical activities on the Incident Commander or Unified Command's behalf;
- Developing and implementing strategies and tactics to achieve incident objectives;
- Organizing the Operations Section to best meet the incident's needs, maintain a manageable span of control, and optimize the use of resources; and
- Supporting IAP development for each operational period.

Planning Section

Planning Section personnel collect, evaluate, and disseminate incident situation information to the Incident Commander or Unified Command and other incident personnel. The staff within this section prepare status reports, display situation information, maintain the status of assigned resources, facilitate the incident action planning process, and prepare the IAP based on input from other sections and Command Staff and guidance from the Incident Commander or Unified Command.

Additional key functions of Planning Section personnel include:

- Facilitating incident planning meetings;
- Recording the status of resources and anticipated resource needs;
- Collecting, organizing, displaying, and disseminating incident status information and analyzing the situation as it changes;
- Planning for the orderly, safe, and efficient demobilization of incident resources; and
- Collecting, recording, and safeguarding all incident documents.

Logistics Section

Logistics Section personnel provide services and support for effective and efficient incident management, including ordering resources. Staff in this section provide facilities, security (of the incident command facilities and personnel), transportation, supplies, equipment maintenance and fuel, food services, communications and IT support, and medical services for incident personnel. Key functions of Logistics Section personnel include:

- Ordering, receiving, storing/housing, and processing incident-related resources;
- Providing ground transportation during an incident, maintaining and supplying vehicles, keeping vehicle usage records, and developing incident traffic plans;
- Setting up, maintaining, securing, and demobilizing incident facilities;
- Determining food and water needs, including ordering food, providing cooking facilities, maintaining food service areas, and managing food security and safety (in cooperation with the Safety Officer);
- Maintaining an incident Communications Plan and acquiring, setting up, issuing, maintaining, and accounting for communications and IT equipment; and
- Providing medical services to incident personnel.

Finance/Administration Section

The Incident Commander or Unified Command establishes a Finance/Administration Section when the incident management activities involve on-scene or incident-specific finance and administrative support services. Finance/Administration staff responsibilities include recording personnel time, negotiating leases and maintaining vendor contracts, administering claims, and tracking and analyzing incident costs. If the Incident Commander or Unified Command establishes this section, staff should closely coordinate with the Planning and Logistics Sections to reconcile operational records with financial documents.

Finance/Administration Section staff support an essential function of ICS in large, complex incidents involving funding originating from multiple sources. In addition to monitoring multiple sources of funds, the section's staff track and report the accrued costs as the incident progresses.

This allows the Incident Commander or Unified Command to forecast needs and request additional funds as needed. Key functions of Finance/Administration Section personnel include:

- Tracking costs, analyzing cost data, making estimates, and recommending cost savings measures;
- Analyzing, reporting, and recording financial concerns resulting from property damage, responder injuries or fatalities at the incident;
- Managing financial matters concerning leases and vendor contracts;
- Managing administrative databases and spreadsheets for analysis and decision making; and
- Recording time for incident personnel and leased equipment.

Intelligence/Investigations Function

The collection, analysis, and sharing of incident-related information are important activities for all incidents. Typically, staff in the Planning Section are responsible for gathering and analyzing operational information and sharing situational awareness, and staff in the Operations Section are responsible for executing tactical activities. However, some incidents involve intensive intelligence gathering and investigative activity, and for such incidents, the Incident Commander or Unified Command may opt to reconfigure intelligence and investigations responsibilities to meet the needs of the incident. This may occur when the incident involves a criminal or terrorist act and/or other non-law-enforcement intelligence/investigations efforts such as epidemiological investigations.

The purpose of the Intelligence/Investigations function is to ensure that intelligence and investigative operations and activities are properly managed and coordinated to:

- Prevent and/or deter potential unlawful activity, incidents, and/or attacks;
- Collect, process, analyze, secure, and disseminate information, intelligence, and situational awareness;
- Identify, document, process, collect, create a chain of custody for, safeguard, examine and analyze, and store evidence or specimens;
- Conduct thorough and comprehensive investigations that lead to the perpetrators' identification and apprehension;
- Conduct missing persons and mass fatality/death investigations;
- Inform and support life safety operations, including the safety and security of all response personnel, by helping to prevent future attacks or escalated impacts; and
- Determine the source or cause of an ongoing incident (e.g., disease outbreak, fire, complex coordinated attack, or cyber incident) to control its impact and/or help prevent the occurrence of similar incidents.

The Incident Commander or Unified Command makes the final determination regarding the scope and placement of the Intelligence/Investigations function within the command structure. Options for its placement are described in Appendix A, Tab 6 Intelligence/Investigations Function.

Common Types of ICS Facilities

The Incident Commander or Unified Command may establish facilities in and around the incident area to house or support incident management functions. The Incident Commander or Unified Command determines the kinds and locations of facilities based on incident needs. Common ICS facilities are described below and illustrated in Figure 5.

Incident Command Post

The ICP is the location of the tactical-level, on-scene incident command organization. This location typically houses the Incident Commander or Unified Command and the Command and General Staffs, but may include other designated incident personnel. Typically, the ICP is located near the incident site and is where on-scene tactical command functions are performed. Personnel conduct incident planning at the ICP, and the Incident Commander or Unified Command may establish an incident communications center at this location.

Staging Areas

The Operations Section Chief may establish staging areas to position and track for resources. A staging area can be any location in which personnel, supplies, and equipment await assignment. Staging areas may include temporary feeding, fueling, and sanitation services. The Operations Section Chief assigns a manager for each staging area who logs in all incoming resources, dispatches resources at a section chief's request, and requests Logistics Section support, as necessary, for resources at the staging area.

Incident Base

An incident base is the site that accommodates primary support activities. An Incident Commander or Unified Command establishes an incident base to house equipment and personnel support operations. An incident base may be co-located with the ICP.

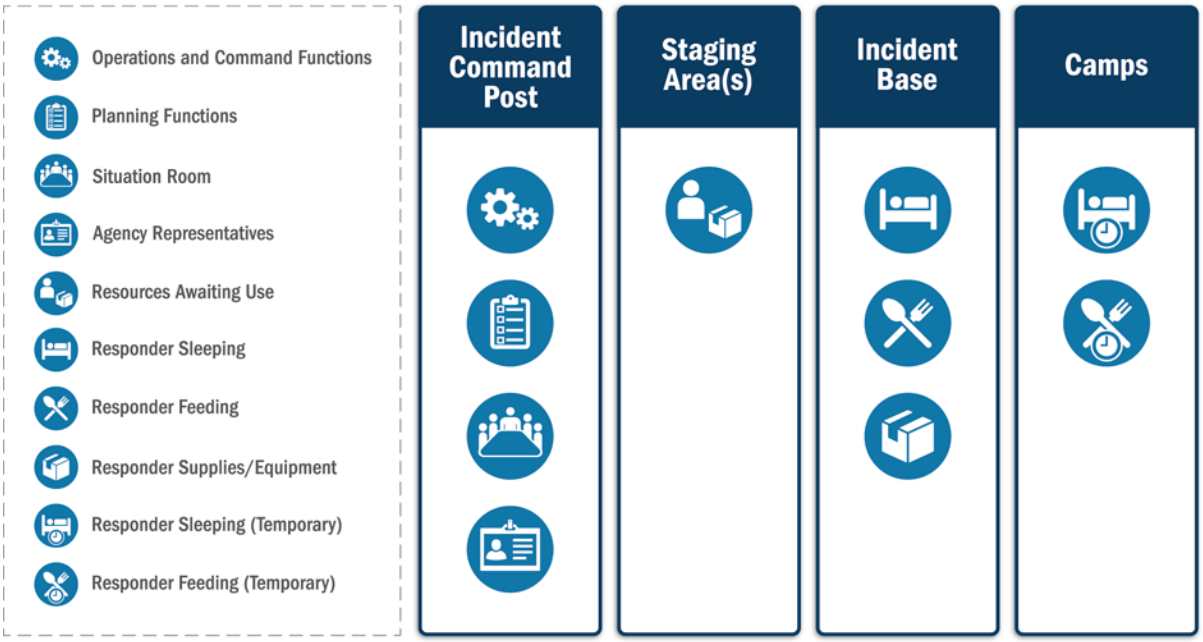


Figure 5: Incident Facilities

Camps

Camps are satellites to an incident base, established where they can best support incident operations. Camps provide support, such as food, sleeping areas, and sanitation, and may also provide minor maintenance and servicing of equipment. Camps are relocated as necessary to meet changing operational needs.

Incident Management Teams

IMTs are rostered groups of ICS-qualified personnel, consisting of an Incident Commander, other incident leadership, and personnel qualified for other key ICS positions. IMTs exist at local, regional, state, tribal, and national levels and have formal notification, deployment, and operational procedures in place. These teams are typed based on team members' qualifications and may be assigned to manage incidents or to accomplish supporting incident-related tasks or functions. When assigned to manage an incident or to support an incident-related task or function, IMTs are typically delegated the authority to act on behalf of the affected jurisdiction or organization.

Delegation of Authority

A delegation of authority is a statement that the authorized jurisdiction/organization official provides to make such delegations to the Incident Commander. It assigns the Incident Commander specific responsibilities and authorities. The delegation of authority typically describes priorities, expectations, constraints, and other considerations or guidelines. Many agencies require the delegating authority to provide a written delegation of authority to the Incident Commander before the Incident Commander may assume command.

Incident Management Assistance Teams

Some IMTs are referred to as Incident Management Assistance Teams (IMAT) to clarify that they support on-scene personnel and/or the affected jurisdiction(s). IMATs may have command and control over certain aspects of response and recovery efforts (e.g., the use of state/Federal assets). Through participation in a Unified Command or a Unified Coordination Group[16] with representatives from local, state, and/or tribal government, they ensure that activities align with local priorities. IMATs exist at various levels of government and within the private sector. Regardless of who owns IMATs or their specific missions, IMATs operate using the principles and practices of ICS.

FEMA IMATs, for example, deploy to incidents or incident-threatened venues, help identify and provide Federal assistance, and coordinate and integrate inter-jurisdictional response in support of an affected state or tribe. FEMA IMATs provide the Federal Government with an early presence at an incident, integrating FEMA's response capabilities into the existing community of emergency management functions.

Incident Complex: Multiple Incident Management within a Single ICS Organization

An incident complex refers to two or more individual incidents located in the same general area and assigned to a single Incident Commander or a Unified Command. When relevant authorities establish an incident complex over several incidents, those incidents become branches or divisions within the incident complex Operations Section. This approach provides potential for future expansion. If any of the incidents within a complex is likely to become a large-scale incident, that incident should be a separate incident with its own ICS organization.

Incident complexes are used in wildfire response when multiple fires occur within close proximity to one another. An incident complex may be managed by either a single Incident Commander or a Unified Command. The following are indicators for use of an incident complex:

- A single Command and General Staff can adequately provide operations, planning, logistics, and finance/administration activities; and
- A combined management approach is likely to achieve staff or logistical support economies.

Area Command

An Area Command is established to oversee multiple concurrent incidents or a very complex incident that requires the establishment of multiple ICS organizations. An Area Command is activated to address competition for resources among multiple ICPs based on the complexity of the incident and incident management span-of-control considerations. Due to the scope of incidents involving Area Commands and the likelihood of cross-jurisdictional operations, Area Commands are frequently established as Unified Area Commands, working under the same principles as a Unified Command.

[16] A Unified Coordination Group is composed of senior leaders representing state, tribal, and Federal interests and, in certain circumstances, local jurisdictions and the private sector. The National Response Framework describes Unified Coordination Groups in greater detail.

Responsibilities of an Area Command include:

- Developing broad objectives for the affected area;
- Coordinating development of incident objectives and strategies for each incident;
- Allocating or reallocating resources as priorities change;
- Ensuring that Incident Commanders and/or Unified Commands properly manage incidents;
- Ensuring effective communications and data coordination;
- Ensuring that incident objectives are met and do not conflict with each other or with agency policies;
- Identifying needs for scarce resources and reporting the needs to Agency Administrators directly or through a MAC Group or an EOC; and
- For incidents that have a recovery dimension, ensuring that short-term recovery is coordinated with the EOC staff to assist in the transition to long-term recovery operations.

Area Command is particularly relevant to situations with several ICPs requesting similar scarce resources. Incidents of different types or without similar resource needs are usually handled as separate incidents. Additional coordination structures, such as EOCs or MAC Groups, may assist with coordinating the resource needs of multiple incidents. The following sections describe these structures. Figure 6 depicts the relationship of an Area Command with a MAC Group and an EOC.

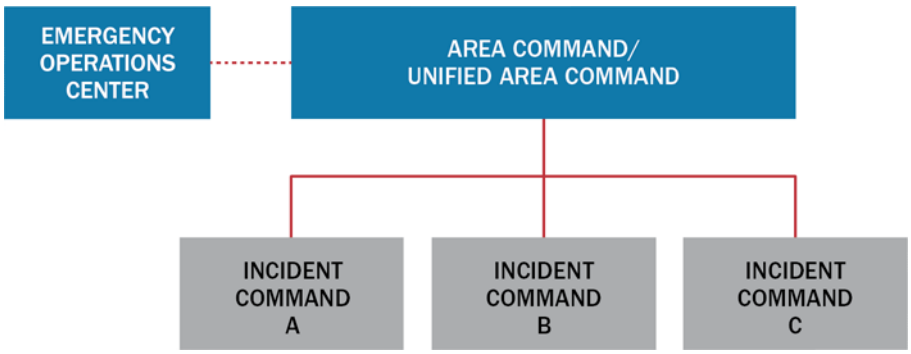


Figure 6: Example of Area Command

Relationship between Area Command, an EOC, and a MAC Group

An Area Command oversees management of multiple incidents, while EOCs coordinate support.

MAC Groups provide policy guidance and strategic direction to Area Command and EOCs.

C. Emergency Operations Centers (EOC)

Jurisdictions and organizations across the Nation use EOCs as important elements in their emergency management programs. EOCs are locations where staff from multiple agencies typically come together to address imminent threats and hazards and to provide coordinated support to incident command, on-scene personnel, and/or other EOCs. EOCs may be fixed locations, temporary facilities, or virtual structures with staff participating remotely.

The purpose, authorities, and composition of the teams that staff EOCs vary widely, but generally, the teams consolidate and exchange information, support decision making, coordinate resources, and communicate with personnel on scene and at other EOCs. EOC personnel may support staff at an ICP, field personnel not affiliated with an ICP (e.g., personnel conducting debris removal or managing a shelter), or staff in another EOC (e.g., staff in a state EOC communicating with staff in a local EOC).

EOC staff may share the load with on-scene incident personnel by managing certain operations, such as emergency shelters or points of distribution. When on-scene incident command is not established, such as in a snow emergency, staff in EOCs may direct tactical operations. Finally, EOC staff may coordinate the efforts of several geographically disparate incidents or activities. In some instances, the incident command or Area Command may be conducted in the EOC.

A jurisdiction or organization may also activate EOC staff to support prevention and protection activities and to find resources to backfill those that the jurisdiction or organization has already deployed.

Primary functions of staff in EOCs, whether virtual or physical, include:

- Collecting, analyzing, and sharing information;
- Supporting resource needs and requests, including allocation and tracking;
- Coordinating plans and determining current and future needs; and
- In some cases, providing coordination and policy direction.

Agencies and departments also have operations centers. However, these organization-specific operations centers differ from multidisciplinary[17] EOCs. Departmental operations center (DOC) staff coordinate their agency or department's activities. While they communicate with other organizations and EOCs and may exchange liaisons with other agencies, DOC staff are primarily inward looking, focusing on directing their own assets and operations. Unlike DOCs, the EOCs addressed in NIMS are inherently multidisciplinary activities.

Bringing representatives from various stakeholder and partner organizations together in EOCs optimizes unity of effort and enables staff to share information, provide legal and policy guidance to on-scene personnel, plan for contingencies, deploy resources efficiently, and generally provide whatever support is required. Determining which organizations are represented

[17] "Multidisciplinary" refers to the assemblage of more than one function (resources and organizations) engaged in emergency management, such as fire prevention and suppression, law enforcement, EMS, public works, and/or others based on the nature of the incident, threat, or hazard.

in EOCs should be accomplished during the emergency operations planning process. Factors to consider include the authorities and responsibilities of various organizations, the resources and information the organizations have or have access to, and the organizations' expertise and relationships. The composition of EOC teams may also vary depending on the nature and complexity of the incident or situation.

Regardless of which organizations are represented, all EOC teams receive oversight from elected and/or appointed officials such as governors, tribal leaders, mayors, and city managers. These individuals may be present in the EOC, but more often provide guidance from elsewhere, either as part of a formal policy group or individually. They typically make decisions regarding priorities and on issues such as emergency declarations, large-scale evacuations, access to extraordinary emergency funding, waivers to ordinances and regulations, and adjudication of scarce resources.

EOC Staff Organizations

EOC teams vary widely. Deciding how to organize the staff in EOCs depends on factors such as the jurisdiction/organization's authorities, staffing, partner and stakeholder agencies represented, EOC physical facilities, communications capabilities, political considerations, and most importantly, the mission.

Regardless of how the EOC staff are organized, they should operate consistently with the NIMS management characteristics.

The following section describes three common ways of organizing EOC teams. Appendix B. EOC Organizations contains more detailed information on each of these structures.

Modular EOC Organizations

The NIMS management characteristic of ***modular organization*** indicates that leaders are responsible for the functions of subordinate positions that are not staffed.

This management characteristic also applies to EOCs. In an EOC where staffing and space are limited, the individual in charge may perform not only the duties of the EOC director, but also the duties of other EOC team members unless or until those other positions are staffed.

ICS or ICS-like Structure

Many jurisdictions/organizations configure their EOCs using the standard ICS organizational structure. The structure is familiar to many people, and it aligns with the on-scene incident organization. Some jurisdictions/organizations use the standard ICS organizational structure but modify certain titles to create an ICS-like organization that distinguishes EOC functions from their field counterparts. Figure 7 depicts an example of such a structure.

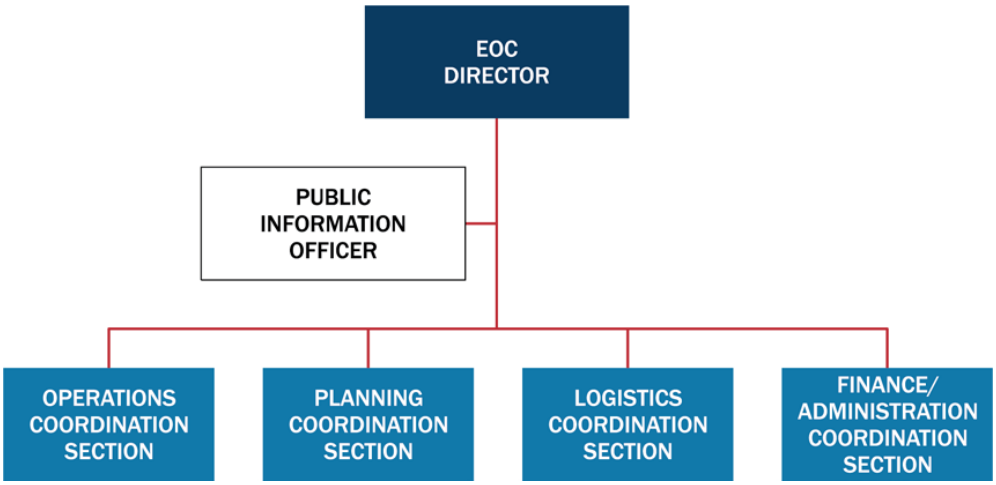


Figure 7: Example of an ICS-like EOC Organization Structure

Incident Support Model (ISM) Structure

Jurisdictions/organizations that focus their EOC team's efforts on information, planning, and resource support may choose to separate the situational awareness function from planning and combine operations and logistics functions into an incident support structure such as the one shown in Figure 8. This organization puts the EOC director in direct contact with those doing situational awareness/information management and streamlines resource sourcing, ordering, and tracking.

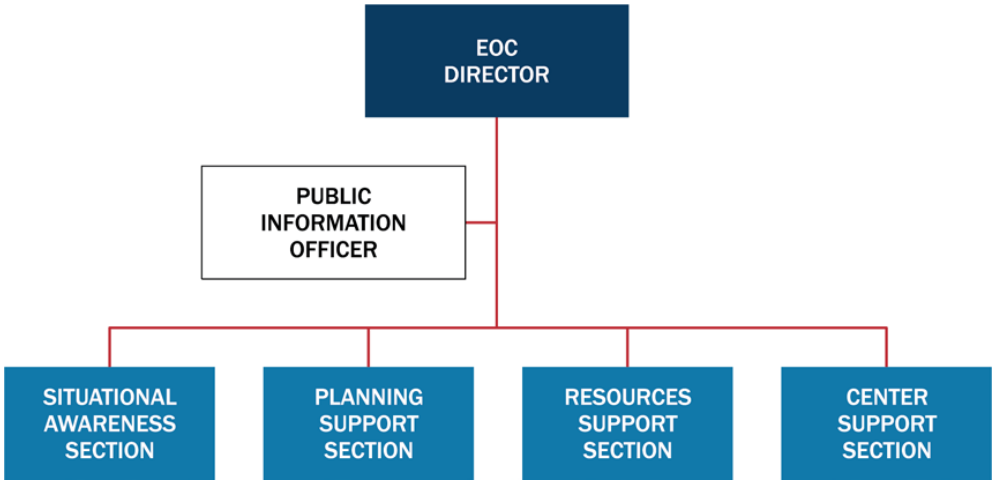


Figure 8: Example of an ISM EOC Structure

Departmental Structure

Jurisdictions/organizations may opt instead to use their day-to-day departmental/agency structure and relationships in their EOC. By operating in the context of their normal relationships, department/agency representatives can function in the EOC with minimal preparation or startup time. Figure 9 provides an example of this kind of EOC organization. In this configuration, the organization's emergency manager or a senior official typically coordinates EOC efforts among the departments and agencies.

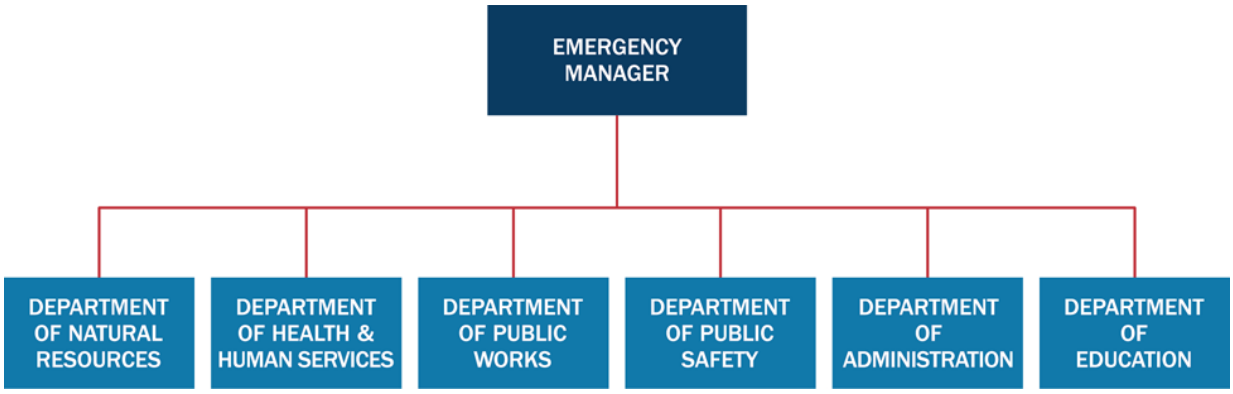


Figure 9: Example of a Departmental EOC Structure

EOC Activation and Deactivation

EOCs are activated for various reasons based on the needs of a jurisdiction, organization, or Incident Commander; the context of a threat; the anticipation of events; or in response to an incident. Circumstances that might trigger EOC activation include:

- More than one jurisdiction becomes involved in an incident and/or the incident involves multiple agencies;
- The Incident Commander or Unified Command indicates an incident could expand rapidly, involve cascading effects, or require additional resources;
- A similar incident in the past led to EOC activation;
- The EOC director or an appointed or elected official directs that the EOC be activated;
- An incident is imminent (e.g., hurricane warnings, slow river flooding, predictions of hazardous weather, elevated threat levels);
- Threshold events described in the emergency operations plan occur; and/or
- Significant impacts to the population are anticipated.

EOCs frequently have multiple activation levels to allow for a scaled response, delivery of the needed resources, and a level of coordination appropriate to the incident.

Normal Operations or Steady State

During normal operations (steady state), emergency management personnel maintain operational readiness by monitoring and assessing potential threats and hazards; conducting routine and ongoing coordination with other departments and agencies; developing and executing plans, training, and exercises; and maintaining facilities and equipment.

Activation Levels

The level of activity within an EOC often grows as the size, scope, and complexity of the incident grow. If the incident management efforts require additional support and coordination, the EOC director may activate additional staff to involve more disciplines, mobilize additional

resources, inform the public, address media inquiries, involve senior elected and appointed officials, and request outside assistance.

Emergency operations plans often specify levels of activation for their EOC, including which organizations and/or personnel will be in the EOC for specific hazards and activation levels. EOC personnel should use the standard NIMS activation level titles listed in Table 2 for communication outside their jurisdiction/organization. Additionally, some organizations may opt to use number or color designations of activation levels for internal communications. When numbers are used, the numbers should reflect the standard NIMS approach of descending numbers meaning higher levels of activation (e.g., full activation should be level 1).

Table 2 lists activation levels, along with criteria for determining the appropriate level. Any of these levels can involve both in-person and off-site personnel coordinating virtually.

Table 2: EOC Activation Levels

Activation Level	Description
3 Normal Operations/ Steady State	• Activities that are normal for the EOC when no incident or specific risk or hazard has been identified • Routine watch and warning activities if the EOC normally houses this function
2 Enhanced Steady-State/ Partial Activation	• Certain EOC team members/organizations are activated to monitor a credible threat, risk, or hazard and/or to support the response to a new and potentially evolving incident
1 Full Activation	• EOC team is activated, including personnel from all assisting agencies, to support the response to a major incident or credible threat

Deactivation

The EOC director deactivates EOC staff as circumstances allow, and the EOC returns to its normal operations/steady state condition. Deactivation typically occurs when the incident no longer needs the support and coordination functions provided by the EOC staff or those functions can be managed by individual organizations or by steady-state coordination mechanisms. EOC leadership may phase deactivation depending on mission needs. EOC staff complete resource demobilization and transfer any ongoing incident support/recovery activities before deactivating. EOC planners normally include after-action review and improvement planning as part of the deactivation planning process.

D. Multiagency Coordination Group (MAC Group)

MAC Groups, sometimes called policy groups, are part of the off-site incident management structure of NIMS. MAC Groups consist of representatives from stakeholder agencies or organizations. They are established and organized to make cooperative multiagency decisions. MAC Groups act as policy-level bodies during incidents, supporting resource prioritization and allocation, and enabling decision making among elected and appointed officials and those responsible for managing the incident (e.g., the Incident Commander). In some instances, EOC staff also carry out this activity.

MAC Groups typically consist of agency administrators, executives, or their designees. Organizations at any level (e.g., local, state, tribal, or Federal) or within any discipline (e.g., emergency management, public health, critical infrastructure, or private sector) may establish a MAC Group. In some jurisdictions, local law or policy may require a MAC Group to authorize additional resources and/or provide guidance to EOC staff and/or incident command.

MAC Groups are primarily responsible for resource prioritization and allocation. Unlike Unified Command, they do not perform incident command functions, nor do they replace the primary functions of operations, coordination, or dispatch organizations. When competition for resources is significant, MAC Groups may relieve the coordination and dispatch organizations of some prioritization and allocation responsibilities.

The composition of MAC Groups is important. Sometimes membership is obvious. Organizations directly affected and whose resources are committed to the incident should be represented. Sometimes, however, organizations that should be MAC Group members are less obvious. These include business organizations such as local chambers of commerce, volunteer organizations such as the American Red Cross, or other organizations with special expertise or knowledge. While these organizations may not have tangible resources or funds to contribute, their relationships, political influence, or technical expertise can be key to the MAC Group's success in supporting incident response and recovery. MAC Group designees should have their respective organization's authorization to represent or commit agency resources and funds for incident activities. MAC Groups typically base their decisions on member consensus. In many cases, a MAC Group can function virtually.

Elected and appointed officials are key players in incident management. They are responsible for the safety and welfare of their constituents and the overall effectiveness of incident management efforts. Governors, tribal leaders, mayors, city managers, and county commissioners, for example, typically comprise the policy level of incident management and provide guidance regarding priorities and strategies for dealing with incident response and recovery. Incident personnel working in EOCs and on scene share the responsibility for keeping elected and appointed officials informed regarding the situation, resource needs, and other pertinent information. Effective communication between these incident personnel and policy-level officials fosters trust and helps ensure that all leaders have the information they need to make informed decisions. MAC Groups provide a way to organize policy-level officials to enhance unity of effort at this senior level.

A MAC Group may need administrative and/or logistical support. In some instances, staff in EOCs provide this support. In other instances, separate organizations are established to support

the MAC Group by meeting its logistical and documentation needs; managing incident-related decision-support information such as tracking critical resources, the situation status, and investigative information; and providing public information to the news media and public.

E. Joint Information System (JIS)

Dissemination of timely, accurate, accessible, and actionable information to the public is important at all phases of incident management. Many agencies and organizations at all levels of government develop and share public information. Jurisdictions and organizations coordinate and integrate communication efforts to ensure that the public receives a consistent and comprehensive message. JISs consist of the processes, procedures, and tools to enable communication to the public, incident personnel, the media, and other stakeholders.

JISs integrate incident information and public affairs into a cohesive organization to provide coordinated and complete information before, during, and after incidents. The JIS mission 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 Incident Commander or Unified Command, EOC director, or MAC Group;
- Advising the Incident Commander or Unified Command, MAC Group, and EOC director concerning public affairs issues that could affect an incident management effort; and
- Addressing and managing rumors and inaccurate information that could undermine public confidence.

JISs cut across the three levels of incident management (on-scene/tactical, center/coordination, policy/strategic) and help ensure coordinated messaging among all incident personnel.

System Description and Components

Public information processes are coordinated before an incident and include the plans, protocols, procedures, and structures used to provide public information. PIOs at all levels of government and within the private and nonprofit sectors and JICs are important supporting elements of the JIS. Key elements of the JIS include the following:

- Interagency coordination and integration;
- Gathering, verifying, coordinating, and disseminating consistent messages;
- Public affairs support for decision makers; and
- Flexibility, modularity, and adaptability.

Public Information Officer

PIOs are key members of ICS and EOC organizations, and they frequently work closely with senior officials represented in MAC Groups. If the PIO position is staffed at both the ICP and a supporting EOC, the PIOs maintain close contact through pre-established JIS protocols. PIOs advise the Incident Commander, Unified Command, or EOC director on public information matters relating to the management of the incident. PIOs also handle inquiries from the media, the public, and elected officials; public information and warnings; rumor monitoring and response; media relations; and other functions needed to gather, verify, coordinate, and

disseminate accurate, accessible, and timely information. Information on public health, safety, and protection is of particular importance. The PIO also monitors the media and other sources of public information and transmits relevant information to the appropriate personnel at the incident, EOC, and/or in a MAC Group.

PIOs create coordinated and consistent messages by collaborating to:

- Identify key information to be communicated to the public;
- Craft clear messages that all can understand, including individuals with Limited English Proficiency, those with disabilities, and others with access and functional needs;[18]
- Prioritize messages to ensure timely delivery of information without overwhelming the audience;
- Verify accuracy of information; and
- Disseminate messages using the most effective means.

Joint Information Center

The JIC is a facility that houses JIS operations, where personnel with public information responsibilities perform essential information and public affairs functions. JICs may be established as standalone coordination entities, at incident sites, or as components of EOCs. Depending on the needs of the incident, an incident-specific JIC may be established at an on-scene location in coordination with local, state, and Federal agencies, or at the national level if the situation warrants. The PIO prepares public information releases for Incident Commander, Unified Command, EOC director, or MAC Group clearance. This helps ensure consistent messages, avoid release of conflicting information, and prevent adverse impact on operations. Jurisdictions and organizations may issue releases related to their policies, procedures, programs, and capabilities; however, these should be coordinated with the incident-specific JIC(s).

An incident should have a single JIC, but the system is flexible and adaptable enough to accommodate multiple physical or virtual JICs. For example, multiple JICs may be needed for a complex incident covering a wide geographic area or multiple jurisdictions. In instances when multiple JICs are activated, staff in the JICs coordinate their efforts and the information they provide. Each JIC has procedures and protocols to communicate and coordinate effectively with the others. When multiple JICs are activated, staff coordinate to determine the final release authority. A national JIC may be used when an incident includes Federal coordination and is expected to go on for some time (e.g., weeks or months) or when the incident affects a large area. JICs can be organized in many ways, depending on the nature of the incident. Table 3 identifies types of JICs.

[18] Messaging should be provided in multiple formats to account for the access and functional needs of individuals who are deaf or hard of hearing, individuals with limited English proficiency, individuals from diverse cultural backgrounds, individuals with cognitive limitations, and individuals who do not use traditional media.

Virtual JIC

When public affairs officials are operating from multiple, dispersed locations, these officials may establish a virtual JIC to connect electronically and perform the coordination functions of a normal JIC.

Table 3: Examples of JIC Types

Type	Characteristics
Incident JIC	• Optimal physical location for local and Incident Commander, Unified Command, or EOC director-assigned PIOs to co-locate • Easy media access (paramount to success) • May be located at an EOC
Virtual JIC	• Established when physical co-location is not feasible • Incorporates technology and communication protocols
Satellite JIC	• Smaller in scale than other JICs • Established to support the primary JIC • Operates under the primary JIC's control
Area JIC	• Supports wide-area, multiple-incident ICS structures • Could be established locally or statewide • Media access is paramount
National JIC	• Typically established for long-duration incidents • Established to support Federal incident management • Staffed by numerous Federal departments and/or agencies • Media access is paramount

Organizational Independence

Organizations participating in incident management retain their independence while collaborating through the JIS to generate common public information. Incident command, EOC leadership, or MAC Group members may be responsible for establishing and overseeing JICs, including establishing processes for coordinating and clearing public communications. In JICs, departments, agencies, organizations, or jurisdictions continue to control information regarding their own programs or policies. Each agency or organization contributes to the overall unified message.

Getting Information to the Public and Stakeholders

In some cases, lives will depend on getting information to the public quickly, and those responsible should take whatever steps are necessary to alert the public. Informing the public and stakeholders during an incident is an ongoing cycle that involves gathering, verifying, coordinating, and disseminating information.

Gathering Information

Gathering information begins the process of getting information to the public and additional stakeholders. Information is collected from various sources, including:

- On-scene command provides ongoing, official information on the incident management effort with much of this information captured in IAPs and situation reports;

- The on-scene PIO reports to the JIC what he or she observes and hears from the news media, elected officials and their staffs, and the public;
- Media monitoring assesses the accuracy and content of news and social media reports and helps identify breaking issues and trends;
- Inquiries from elected and appointed officials and the general public can point to the specific concerns of those in the affected areas; and
- Staff in EOCs generate information relating to the situation status and/or mass care, recovery, or other assistance available to the public.

Verifying Information

The next step in the process is to verify the accuracy of the information collected. PIOs representing different agencies have access to different information sources. In addition to verifying their information through standard means, participation in the JIC provides PIOs from different agencies the opportunity to compare notes and deconflict information they have gathered from various sources.

Coordinating Information

The next step is to coordinate with other public information personnel who are part of the JIS. This includes both those represented in the JIC and those working from another location that is part of the JIS. Coordinating information involves the following:

- ***Establishing key message(s)***. After gathering information, JIC staff craft unified messages that address informational needs which are prioritized according to the overall local, state, tribal, territorial, and Federal incident management priorities and strategies. The mission includes getting accurate, consistent information to the right people at the right time so they can make informed decisions.
- ***Obtaining approval or clearance from those with authority***. This helps ensure that the information is consistent and accurate; however, the approval process should be streamlined so that information can be released in a timely manner.

Disseminating Information

The final step in the process is to disseminate information to the public and stakeholders. In some emergencies, many modes of communication may not be available. Press releases, phone calls, and interviews are traditional means of getting information to the news media. In some cases, personal visits or town meetings may be the most effective means of reaching key audiences. Local, state, tribal, and Federal systems such as the Integrated Public Alert and Warning System (IPAWS), the Emergency Alert System (EAS), and the National Terrorism Advisory System (NTAS) facilitate communication with the public. Social media outlets are an important method of reaching the public directly; such outlets provide flexibility for targeting specific audiences or communicating when traditional media is unavailable, as in a power outage. These outreach efforts can be supported by providing talking points and fliers to the PIO and other community leaders.

Monitoring news and social media outlets helps identify rumors, inaccuracies, or information gaps. Important inaccuracies should be addressed before the media incorrectly reports them a second time.

Public Information Communications Planning

Well-developed and coordinated public information, education, and communications plans and strategies make it possible to share public safety information, including lifesaving measures or evacuation routes through threat and alert systems in a timely, consistent, accurate, and accessible manner. Plans should include processes, protocols, and procedures for developing draft news releases; media lists; and contact information for elected/appointed officials, community leaders, private sector organizations, and public service organizations. Planners should ensure their information communication plans facilitate disseminating public information. Public information communications should also be included in training and exercises.

F. Interconnectivity of NIMS Command and Coordination Structures

NIMS structures enable incident managers across the Nation—from the Incident Commander or Unified Command in the field to the leadership in FEMA's National Response Coordination Center (NRCC)—to manage an incident in a unified, consistent manner. The interconnectivity of NIMS structures allows personnel in diverse geographic areas with differing roles and responsibilities and operating within various functions of ICS and/or EOCs to integrate their efforts through a common set of structures, terminology, and processes.

When an incident occurs or threatens, local incident personnel respond, using NIMS principles and structures to frame their activities. If the incident is or becomes large or complex, EOCs activate. EOC staff receive senior-level guidance from MAC Groups. Establishing a JIC helps ensure coordinated and accurate public messaging.

If personnel cannot find resources locally, they may obtain them through mutual aid agreements from neighboring jurisdictions or from state, tribal, territorial, or interstate sources. The state EOC may activate to support incident management information and resource needs. Qualified personnel can be requested using standard vocabulary, so that the requesting jurisdictions understand exactly what they will receive. When the resources (personnel, teams, facilities, equipment, or supplies) reach the incident, incident personnel can incorporate them seamlessly using common, standard systems (e.g., ICS, JIS).

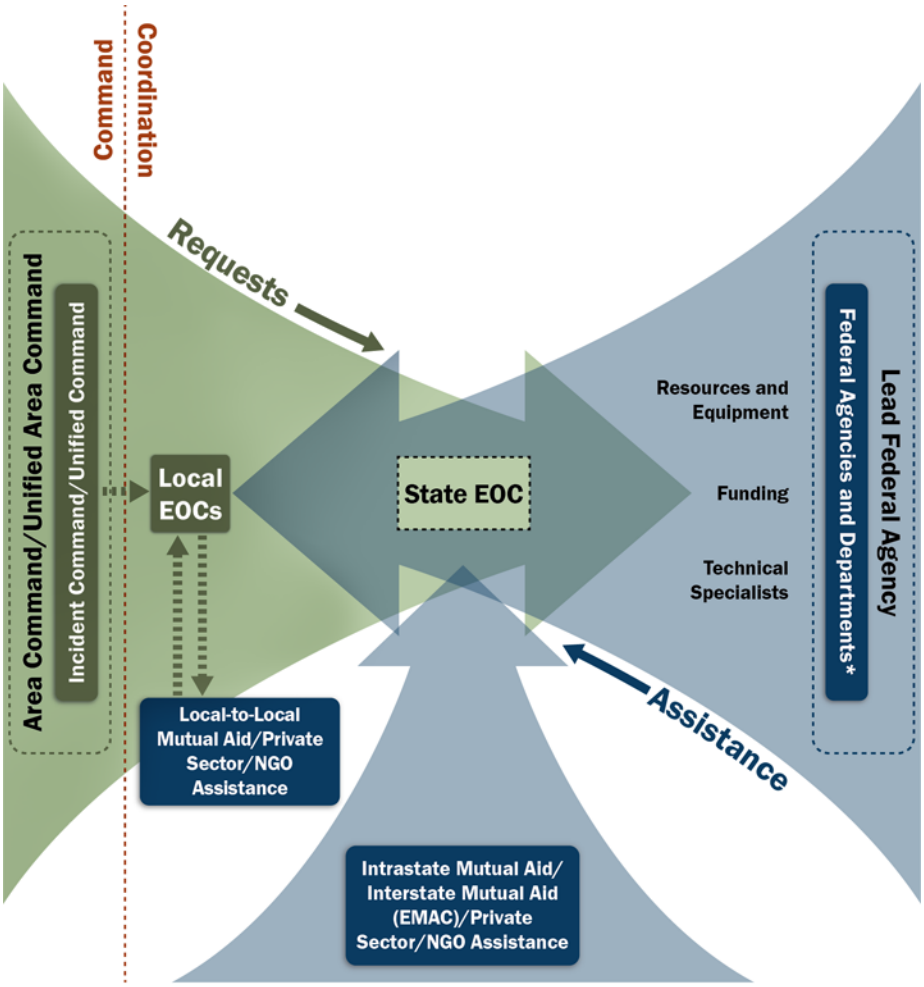
Federal Support to Response Activities

Most incidents are resolved using the coordination mechanisms described above; however, some major incidents may need assistance from the Federal Government. The Federal Government maintains a wide range of capabilities and resources needed to address domestic incidents. NIMS coordinating structures enable Federal departments and agencies to cooperate with one another and with local, state, tribal, territorial, and insular area governments, community members, and the private sector.

The Federal Government becomes involved with a response:

- When state governors or tribal leaders request Federal assistance and the requests are approved;
- When Federal interests are involved; or
- As statute authorizes or requires.

Accordingly, in some instances, the Federal Government plays a supporting role to local, state, tribal, or territorial governments by providing Federal assistance to the affected jurisdictions. For example, the Federal Government provides assistance when the President declares an emergency or major disaster under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). Figure 10 depicts the integration of the Federal Government when it is playing a primarily support role.



*Some Federal agencies (U.S. Coast Guard, Environmental Protection Agency, etc.) have statutory responsibility for response and may coordinate and/or integrate directly with affected jurisdictions. During responses conducted under Stafford Act declarations, FEMA establishes a Joint Field Office (JFO) to coordinate Federal response activities.

Figure 10: Federal Support to Response Activities

In other instances, the Federal Government plays a leading role in the response, such as when incidents occur on Federal property (e.g., national parks) or when the Federal Government has primary jurisdiction (e.g., an ongoing terrorist threat or attack or a major oil spill). Various Federal departments and agencies have their own authorities and responsibilities for responding to or assisting with incidents. This means that, depending on the incident, different Federal departments or agencies lead coordination of the Federal Government's response. For example:

- FEMA leads and coordinates Federal response and assistance when the President declares a major disaster or emergency under the Stafford Act;
- The Department of Health and Human Services (HHS) leads Federal public health and medical response to public health emergencies and incidents;
- The location of a major hazardous material spill determines whether the Environmental Protection Agency or the United States Coast Guard serves as the lead Federal agency; and

- The Attorney General and Director of the Federal Bureau of Investigation (FBI) execute their lead responsibility for the law enforcement response to, and criminal investigation of, terrorist threats or incidents.

Lead Federal agencies are typically supported by other agencies that bring their relevant capabilities to bear.

IV. Communications and Information Management

Incident personnel rely on flexible communications and information systems to obtain and provide accurate, timely, and relevant information. Establishing and maintaining situational awareness and ensuring accessibility and voice and data interoperability are the principal goals of the Communications and Information Management component. Properly planned, established, and applied communications facilitate information dissemination among command and support elements and cooperating jurisdictions and organizations.

This section addresses both information sharing, which is the responsibility of all personnel, and the communications systems that support information sharing, which typically fall to staff in the Logistics Section in ICS and logistics or center support staff in EOCs. To maintain situational awareness, incident personnel update incident information continually by gathering, collating, synthesizing, and disseminating incident information to and from all appropriate parties. This information flow is facilitated through developing and using common plans and interoperable equipment, processes, standards, and architectures. During an incident, this integrated, familiar approach links all incident personnel, whether on scene, in an EOC, or in another support location, to maintain communications connectivity and situational awareness. Communications and information management planning address the incident-related policies, equipment, data architecture, systems, standards, and training necessary to achieve interoperable communications.

The following principles of communications and information management support incident managers in maintaining a constant flow of information during an incident. The key principles are (1) Interoperability; (2) Reliability, Scalability, and Portability; (3) Resilience and Redundancy; and (4) Security.

Interoperability: Interoperable communications systems enable personnel and organizations to communicate within and across jurisdictions and organizations via voice, data, and video systems in real time. Interoperability plans address governance, standard operating procedures (SOP), technology, training and exercises, and usage during routine operations, as well as major incidents.

Reliability, Scalability, and Portability: Communications and information systems should be reliable and scalable to function in any type of incident. This means they should be suitable for use within a single jurisdiction or agency, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement. Regular use of communications and information systems helps ensure that they are familiar, applicable, and acceptable to users; readily adaptable to new technology; and reliable in any situation. Scalability means that systems can be expanded to support any situation—including a major incident or several incidents that involve numerous responders and support personnel from multiple jurisdictions and organizations—and that the number of users on a system can be readily increased.

Portable technologies and equipment ensure the effective integration, transport, and deployment of communications systems. Portability includes the standardized assignment of radio channels across jurisdictions, which allows incident personnel to participate in an incident outside their jurisdiction and still use familiar equipment.

Resilience and Redundancy: Resilience and redundancy in communications help to ensure the uninterrupted flow of information. Resilience is the ability of systems to withstand and continue to perform after damage or loss of infrastructure. Redundancy is achieved through the duplication of services. It enables the continuity of communication when primary communications capabilities suffer damage through diverse alternative methods.

Security: Some information communicated from, among, and to incident personnel is sensitive. Additionally, EOC and incident personnel may have access to critical assets, such as industrial control systems, that could cause widespread impacts if compromised. Incident personnel should work with IT and security experts to incorporate data, network, and systems protection best practices into incident communications and data sharing. Intelligence/investigations function staff, for example, may discuss sensitive, personally identifiable, or classified information and must shield this information in accordance with applicable law. Incident communications and information sharing should comply with data protection and privacy laws.

A. Communications Management

The communications management practices and considerations described below help incident personnel from different disciplines, jurisdictions, organizations, and agencies communicate with each other effectively during incidents.

Standardized Communication Types

Incident personnel and their affiliated organizations should use standard communications types, including:

- ***Strategic***: High-level directions, including resource priority decisions, roles and responsibilities determinations, and overall incident management courses of action.
- ***Tactical***: Communications between on-scene command and tactical personnel and cooperating agencies and organizations.
- ***Support***: Coordination in support of strategic and tactical communications (e.g., communications among hospitals concerning resource ordering, dispatching, and tracking; traffic and public works communications).
- ***Public***: Alerts and warnings, press conferences.

Policy and Planning

Coordinated communications policy and planning provides the basis for effective communications and information management. Careful planning determines what communications systems and platforms personnel will use, who can use them, what information is essential in different environments, the technical parameters of all equipment and systems, and other relevant considerations. As technologies change and information exchange methods improve, communications management plans and procedures should also evolve.

All stakeholders, including NGOs and private sector and critical infrastructure owners, should be involved in formulating communications plans and strategies which should be thorough, integrated, and interoperable. Technology and equipment standards also are shared with stakeholders to improve interoperability.

Planners should incorporate sound communication management policies and plans into emergency operations plans and other appropriate plans. Plans should include the following aspects of communications and information management:

- Information needs and potential sources for this information;
- Guidance, standards, and tools to integrate information with partner organizations;
- Procedures, protocols, and networks to release warnings, incident notifications, public communications, and other critical information;
- Mechanisms and protocols for notifying other levels of government and partner organizations;

- Protocols for the effective and efficient use of information management technologies (e.g., computers, networks, and information-sharing mechanisms) to integrate all command, coordination, and support functions; and
- Guidance and mechanisms to ensure that incident messaging is simultaneously accessible to all people, including those who have limited proficiency in English, disabilities, and others who have access and functional needs.

Agreements

All parties identified in a jurisdiction's emergency operations plan should have agreements in place to ensure that the communications elements described in plans and procedures are in effect at the time of an incident. Agreements typically specify the communications systems and platforms that the parties agree to use or through which they intend to share information. These agreements typically include connection of networks, data format standards, and cybersecurity agreements.

Equipment Standards

Communication equipment that personnel use during incident management often consists of components and systems connected through common interfaces, many of which rely on the private sector to provide their operational backbone. Public/private communications systems and associated equipment should be regularly enhanced and updated, as their maintenance is essential to effective incident management. When developing communications systems and equipment standards, personnel should consider:

- The range of conditions under which personnel will use the systems;
- The range of personnel who might potentially use them;
- Current nationally recognized communications standards;[19] and
- The need for durable equipment.

Training

Training and exercises that employ interoperable systems and equipment enable personnel to understand their capabilities and limitations before an incident.

[19] Standards-developing organizations such as the American National Standards Institute (ANSI) and the National Fire Protection Association (NFPA) regularly update and publish communications standards.

B. Incident Information

During an incident, personnel need timely and accurate information to make decisions. Information is used for many functions within ICS, EOCs, MAC Groups, and JISs, including:

- Aiding in planning;
- Communicating with the public, including emergency protective measures;
- Determining incident cost;
- Determining the need for additional involvement of NGO or private sector resources;
- Identifying safety issues; and
- Resolving information requests.

Incident Reports

Incident reports enhance situational awareness and help ensure that personnel have easier access to essential information. Types of reports that provide essential information regarding the incident include:

- ***Situation Reports (SITREP)***: Reports typically produced and distributed on a regular and recurring basis that contain incident details. SITREPs offer a snapshot of the incident status during the past operational period and contain confirmed or verified information regarding the explicit details (who, what, when, where, and how) relating to the incident.
- ***Status Reports***: Reports, such as spot reports, that include vital and/or time-sensitive information outside regularly scheduled situation reports. Status reports are typically function-specific and less formal than SITREPs.

Standardizing the information contained in incident notification, situation, and status reports within and across jurisdictions and organizations facilitates information processing; however, the standardization should not prevent the collection or dissemination of information unique to a reporting organization. Transmitting data in a common format enables other jurisdictions and organizations to anticipate, and rapidly find and act on, specific incident information.

Incident Action Plans

In addition to incident reports, personnel can also improve situational awareness and better understand incident objectives and tactics by referring to IAPs. IAPs contain the incident objectives that the Incident Commander or Unified Command establishes and address tactics for the planned operational period, generally 12 to 24 hours. See Appendix A, ICS Tab 8 for details regarding the incident action planning process.

Data Collection and Processing

Personnel should collect data in a manner that observes standard data collection techniques and definitions, analyze the data, and share it through the appropriate channels. Standardized sampling and data collection enables reliable analysis and improves assessment quality.

Leaders in ICS organizations, in EOCs, on MAC Groups, and public affairs personnel all rely on accurate and timely information. Data collection and processing include the following standard elements: initial size up/rapid assessment, data collection plans, validation, analysis, dissemination, and updating.

Initial Size-Up/Rapid Assessment

The official who is the first to arrive at the scene of an incident assesses the situation and provides his/her findings to dispatch or other incident support organizations. Staff in these organizations then use this information to assign resources and make other incident-related decisions.

Data Collection Plan

The Incident Commander, Unified Command, or EOC director may establish a data collection plan to standardize the recurring process of collecting incident information. A data collection plan is typically a matrix that describes what essential elements of information (EEI)—information items required for informed decision making—personnel will collect. The data collection plan lists sources, methods, units of measure, and schedules for collecting various items.

The EEI should be defined prior to developing a data collection plan. EEI typically includes items such as:

- Incident area boundaries/access points;
- Jurisdictional boundaries;
- Social/economic/political impacts;
- Impact to health of the population;
- Transportation system status;
- Communications system status;
- Hazard-specific information;
- Significant weather;
- Seismic or other geophysical data;
- Critical facility status;
- Aerial reconnaissance activity status;
- Disaster/emergency declaration status;
- Planned or upcoming activities; or
- Donations.

Personnel accomplish data gathering using a wide variety of methods:

- Obtaining data from 911 calls from public safety telecommunicators or from dispatch systems;
- Monitoring radio, video, and/or data communications among responders;
- Reading SITREPs;
- Using technical specialists such as National Weather Service representatives;
- Receiving reports from field observers, ICPs, Area Commands, MAC Groups, DOCs, and other EOCs;
- Deploying information specialists to EOCs, other facilities, and operational field offices;
- Analyzing relevant geospatial products; and
- Monitoring print, online, broadcast, and social media.

Validation

Staff responsible for situational awareness review data to determine if it is incomplete, inaccurate, embellished, outdated, or misleading. Personnel should use a variety of sources to validate data.

Analysis

Situational awareness staff analyze validated data to determine its implications for incident management and to turn raw data into information that is useful for decision making. Analysis addresses the incident's information needs by breaking those information needs into smaller, more manageable elements and then addressing those elements. Personnel should base their analysis on a thorough understanding of the problems and the situation. Personnel should provide timely and objective analysis and be cognizant of missing or unknown data.

Dissemination

Once personnel have collected and validated the incident data, they share it with others, in alignment with applicable data dissemination laws and policies. Personnel should disseminate incident information in a timely and accurate way, with the goals of enhancing situational awareness and encouraging effective coordination.

Updating

Informational accuracy and completeness can help incident managers make sound decisions. Personnel can develop situational awareness by continually monitoring, verifying, integrating, and analyzing relevant elements of data and information.

C. Communications Standards and Formats

Common Terminology, Plain Language, Compatibility

Common Terminology

The use of common terminology helps incident personnel from different disciplines, jurisdictions, organizations, and agencies communicate and effectively coordinate activities.

Plain Language

Using plain language and clear text, not codes, in incident management is a matter of public safety, especially the safety of incident personnel and those affected by the incident.

Personnel should use plain language in all communications between organizational elements during an incident, whether oral or written, to help ensure that personnel are disseminating information in a timely and clear manner and that all intended recipients understand. Personnel should avoid using acronyms or jargon unique to an agency, organization, or jurisdiction during incidents that involve multiple jurisdictions or organizations.

Data Interoperability

Personnel should plan, establish, and apply communications protocols to enable the dissemination of information among management, command, and support elements and cooperating jurisdictions and organizations. Elements of compatible information management include:

- ***Data Communication Protocols***: Procedures and protocols for communications (to include voice, data, geospatial information, internet use, and data encryption) to use or share information. This includes structuring and sharing information consistently with the National Information Exchange Model (NIEM) (http://www.niem.gov).
- ***Data Collection Protocols***: Establishing multidisciplinary and/or multijurisdictional procedures and protocols, such as use of the United States National Grid, before an incident allows for standardized data collection and analysis.
- ***Encryption or Tactical Language***: When necessary, incident management personnel and their affiliated organizations should have methodology and systems in place to encrypt information to maintain security. Although plain language is appropriate during most incidents, tactical language is occasionally warranted due to the nature of the incident (e.g., during an ongoing terrorist event). In such instances, guidance on the appropriate use of specialized encryption and tactical language should be incorporated in an incident-specific communications plan.

United States National Grid

The United States National Grid is a point and area location reference system that FEMA and other incident management organizations use as an alternative to latitude/longitude. The National Grid is simple to apply to support risk assessment, planning, response, and recovery operations. Individuals, public agencies, voluntary organizations, and commercial enterprises can use the National Grid within and across diverse geographic areas and disciplines. The use of the National Grid promotes consistent situational awareness across all levels of government, disciplines, threats, and hazards, regardless of an individual or program's role.

Technology Use and Procedures

Personnel use technological tools before, during, and after incidents as a mechanism to offer increased situational awareness to jurisdictions/organizations involved in the incident and/or to the public. Examples of these technologies include:

- Radio and telephone systems;
- Public warning and notification systems;
- Hardware, software, and internet-based systems and applications (including Geographic/Geospatial Information Systems [GIS] and incident management software); and
- Social media.

Incident personnel should establish procedures for using technology and other tools to benefit from these valuable communications resources. Information that personnel gain or share during an incident through these applications should follow planned and standardized methods and generally conform to overall information sharing standards, procedures, and protocols.

Social Media

Social media presents unique considerations for incident management at all levels and provides a set of tools that can facilitate:

- Monitoring and gathering information and firsthand accounts of incident impacts;
- Distributing public information and warning;
- Producing maps and incident visualizations; and
- Matching available information, services, and resources to identified needs.

Using Social Media for Situational Awareness

Social media provides innovative ways of gathering data to achieve situational awareness. Monitoring of spikes or trends in social media by fusion centers, law enforcement, public health, or other information monitoring systems may enhance situational awareness or provide early indication of emerging issues. As with all data, incident personnel use data validation processes to filter and determine the accuracy of information gained via social media.

Using Social Media for Disseminating Information

Increasingly, the public expects incident management personnel to use social media to communicate necessary information. When using social media to disseminate information, considerations for incident managers include:

- Identifying the intended audiences and what types of information to share;
- Determining if they wish to solicit feedback or responses; and
- The potential time delay before survivors receive the message.

These decisions help incident managers determine which social media platforms they should use, the frequency and configuration of messages, and assignments and staffing needs. As with other public information, personnel should follow standard release protocols and ensure accessibility.

Information Security/Operational Security

The need for confidentiality sometimes complicates sharing information. This can be particularly pronounced when sharing intelligence within the law enforcement community and with the emergency management, fire, public health, and other communities. Access to certain restricted or classified information depends on applicable law, as well as an individual's security clearance and need to know.

V. Conclusion

The Nation faces complex and evolving threats and hazards. The varied capabilities and resources of diverse organizations across the Nation are a tremendous asset, but applying these capabilities in a coordinated manner can be challenging. Together, the components of NIMS enable nationwide unity of effort through shared vocabulary, systems, and processes to deliver the capabilities described in the National Preparedness System. NIMS concepts, principles, procedures, structures, and processes link the Nation's responders together, enabling them to meet challenges beyond the capacity of any single jurisdiction or organization.

NIMS is a living document that evolves to capitalize on new opportunities and meet emerging challenges. Incident management stakeholders continue to build on this foundation by developing supporting tools, guidance, education, training, and other resources. FEMA will continue to collect stakeholder feedback, best practices, and lessons learned to drive revisions to NIMS. This includes reviewing after-action reports from real-world incidents and exercises, technical assistance interactions, and focused data collection efforts. In addition to this ongoing feedback, FEMA will conduct quadrennial reviews to evaluate NIMS's consistency with existing and new policies, evolving conditions, and experience gained from its use.

America's preparedness work is never finished. Although the Nation is safer, stronger, and better prepared than it was a decade ago, the commitment to safeguard the Nation against its greatest risks, now and for decades to come, remains resolute. By bringing the whole community together now to address future needs, the Nation will continue to improve its preparedness to face whatever challenges unfold.

VI. Glossary

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

Access and Functional Needs: Individual circumstances requiring assistance, accommodation, or modification for mobility, communication, transportation, safety, health maintenance, etc., due to any temporary or permanent situation that limits an individual's ability to take action in an emergency.

Agency: A government element with a specific function offering a particular kind of assistance.

Agency Administrator/Executive: The official responsible for administering policy for an agency or jurisdiction.

Agency Representative: A person assigned by a primary, assisting, or cooperating local, state, tribal, territorial, or Federal Government agency, or nongovernmental or private organization, who has authority to make decisions affecting that agency's or organization's participation in incident management activities following appropriate consultation with that agency's leadership.

Area Command: An organization that oversees the management of multiple incidents or oversees the management of a very large or evolving situation with multiple ICS organizations. See *Unified Area Command*.

Assigned Resource: A resource that has been checked in and assigned work tasks on an incident.

Assignment: A task given to a person or team to perform based on operational objectives defined in the IAP.

Assistant: A title for subordinates of principal Command Staff and EOC director's staff positions. The title indicates a level of technical capability, qualification, 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.

Authority Having Jurisdiction: An entity that has the authority and responsibility for developing, implementing, maintaining, and overseeing the qualification process within its organization or jurisdiction. This may be a state or Federal agency, training commission, NGO, private sector company, or a tribal or local agency such as a police, fire, or public works department. In some cases, the AHJ may provide support to multiple disciplines that collaborate as a part of a team (e.g., an IMT).

Available Resource: A resource assigned to an incident, checked in, and available for assignment.

Badging: The assignment of physical incident-specific credentials to establish legitimacy and permit access to incident sites. See *Credentialing*.

Base: See *Incident Base*.

Branch: The organizational level having functional or geographical responsibility for major aspects of incident operations. A branch falls between the Section Chief and the division or group in the Operations Section, and between the section and units in the Logistics Section. Branches are identified by Roman numerals or by functional area.

Camp: A geographical site within the general incident area (separate from the Incident Base) that is equipped and staffed to provide sleeping, food, water, and sanitary services to incident personnel.

Certification: The process of authoritatively attesting that individuals meet qualifications established for key incident management functions and are, therefore, qualified for specific positions.

Chain of Command: The orderly line of authority within the ranks of incident management organizations.

Check-In: The process through which resources first report to an incident. All responders, regardless of agency affiliation, report in to receive an assignment in accordance with the Incident Commander or Unified Command's established procedures.

Chief: The ICS title for individuals responsible for the management of functional sections: Operations, Planning, Logistics, and Finance/Administration.

Clear Text: Communication that does not use codes. See *Plain Language*.

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

Command Staff: A group of incident personnel that the Incident Commander or Unified Command assigns to support the command function at an ICP. Command staff often include a PIO, a Safety Officer, and a Liaison Officer, who have assistants as necessary. Additional positions may be needed, depending on the incident.

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

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

Core Capability: An element defined in the National Preparedness Goal as necessary to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

Credentialing: Providing documentation that identifies personnel and authenticates and verifies their qualification for a particular position. See *Badging*.

Critical Infrastructure: Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such assets, systems, or networks

would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Delegation of Authority: A statement that the agency executive delegating authority and assigning responsibility provides to the Incident Commander. The delegation of authority can include priorities, expectations, constraints, and other considerations or guidelines, as needed.

Demobilization: The orderly, safe, and efficient return of an incident resource to its original location and status.

Departmental Operations Center: An operations or coordination center dedicated to a single, specific department or agency. The focus of a DOC is on internal agency incident management and response. DOCs are often linked to and/or physically represented in a combined agency EOC by an authorized agent(s) for the department or agency.

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

Director: The ICS title for individuals responsible for supervision of a branch. Also, an organizational title for an individual responsible for managing and directing the team in an EOC.

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 organizational level having responsibility for operations within a defined geographic area. Divisions are established when the number of resources exceeds the manageable span of control of the Section Chief. See *Group*.

Emergency: Any incident, whether natural, technological, or human-caused, that necessitates responsive action to protect life or property.

Emergency Management Assistance Compact: A congressionally ratified agreement that provides form and structure to interstate mutual aid. Through EMAC, a disaster-affected state can request and receive assistance from other member states quickly and efficiently, resolving two key issues up front: liability and reimbursement.

Emergency Operations Center: The physical location where the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction.

Emergency Operations Plan: A plan for responding to a variety of potential hazards.

Emergency Support Function: The grouping of governmental and certain private sector capabilities into an organizational structure to provide capabilities and services most likely needed to manage domestic incidents.

Essential Elements of Information: Important and standard information items, which support timely and informed decisions.

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

Event: See *Planned Event*.

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

Finance/Administration Section: The ICS Section responsible for an incident's administrative and financial considerations.

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

Group: An organizational subdivision 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 area. See *Division*.

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

Incident: An occurrence, natural or manmade, that necessitates a response to protect life or property. In this document, the word "incident" includes planned events as well as emergencies and/or disasters of all kinds and sizes.

Incident Action Plan: An oral or written plan containing the objectives established by the Incident Commander or Unified Command and addressing tactics and support activities for the planned operational period, generally 12 to 24 hours.

Incident Base: A location where personnel coordinate and administer logistics functions for an incident. There is typically only one base per incident. (An incident name or other designator is added to the term *Base*.) The ICP may be co-located with the Incident Base.

Incident Command: The ICS organizational element responsible for overall management of the incident and consisting of the Incident Commander or Unified Command and any additional Command Staff activated.

Incident Command Post: The field location where the primary functions of incident command are performed. The ICP may be co-located with the Incident Base or other incident facilities.

Incident Command System: A standardized approach to the command, control, and coordination of on-scene incident management, providing a common hierarchy within which personnel from multiple organizations can be effective. ICS is the combination of procedures, personnel, facilities, equipment, and communications operating within a common organizational structure, designed to aid in the management of on-scene resources during incidents. It is used for all kinds of incidents and is applicable to small, as well as large and complex, incidents, including planned events.

Incident Commander: The individual responsible for on-scene incident activities, including developing incident objectives and ordering and releasing resources. The Incident Commander has overall authority and responsibility for conducting incident operations.

Incident Complex: Two or more individual incidents located in the same general area and assigned to a single Incident Commander or Unified Command.

Incident Management: The broad spectrum of activities and organizations providing operations, coordination, and support applied at all levels of government, using both governmental and nongovernmental resources to plan for, respond to, and recover from an incident, regardless of cause, size, or complexity.

Incident Management Assistance Team: A team of ICS-qualified personnel, configured according to ICS, that deploy in support of affected jurisdictions and/or on-scene personnel.

Incident Management Team: A rostered group of ICS-qualified personnel consisting of an Incident Commander, Command and General Staff, and personnel assigned to other key ICS positions.

Incident Objective: A statement of an outcome to be accomplished or achieved. Incident objectives are used to select strategies and tactics. Incident objectives should be realistic, achievable, and measurable, yet flexible enough to allow strategic and tactical alternatives.

Incident Personnel: All individuals who have roles in incident management or support, whether on scene, in an EOC, or participating in a MAC Group.

Information Management: The collection, organization, and control over the structure, processing, and delivery of information from one or more sources and distribution to one or more audiences who have a stake in that information.

Intelligence/Investigations Function: Efforts to determine the source or cause of the incident (e.g., disease outbreak, fire, complex coordinated attack, or cyber incident) in order to control its impact and/or help prevent the occurrence of similar incidents. In ICS, the function may be accomplished in the Planning Section, Operations Section, Command Staff, as a separate General Staff section, or in some combination of these locations.

Interoperability: The ability of systems, personnel, and equipment to provide and receive functionality, data, information, and/or services to and from other systems, personnel, and equipment, between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together.

Joint Field Office: The primary Federal incident management field structure. The JFO is a temporary Federal facility that provides a central location for the coordination of local, state, tribal, and Federal governments and private sector and NGOs with primary responsibility for response and recovery.

Joint Information Center: A facility in which personnel coordinate incident-related public information activities. The JIC serves as the central point of contact for all news media. Public information officials from all participating agencies co-locate at, or virtually coordinate through, the JIC.

Joint Information System: A structure that integrates overarching incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely, and complete information during crisis or incident operations.

Jurisdiction: Jurisdiction has two definitions depending on the context:

- ***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., local, state, tribal, territorial, and Federal boundary lines) and/or functional (e.g., law enforcement, public health).
- ***A political subdivision*** (e.g., municipality, county, parish, state, Federal) with the responsibility for ensuring public safety, health, and welfare within its legal authorities and geographic boundaries.

Kind: As applied to incident resources, a class or group of items or people of the same nature or character or classified together because they have traits in common.

Leader: The ICS title for an individual who is responsible for supervision of a unit, strike team, resource team, or task force.

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

Local Government: Public entities responsible for the security and welfare of a designated area as established by law. 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; a tribe or authorized tribal entity, or in Alaska, a Native Village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity.

Logistics: The process and procedure for providing resources and other services to support incident management.

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

Management by Objectives: A management approach, fundamental to NIMS, that involves (1) establishing objectives, e.g., specific, measurable and realistic outcomes to be achieved; (2) identifying strategies, tactics, and tasks to achieve the objectives; (3) performing the tactics and tasks and measuring and documenting results in achieving the objectives; and (4) taking corrective action to modify strategies, tactics, and/or performance to achieve the objectives.

Manager: The individual within an ICS organizational unit assigned specific managerial responsibilities (e.g., Staging Area Manager or Camp Manager).

Mission Area: One of five areas (Prevention, Protection, Mitigation, Response, and Recovery) designated in the National Preparedness Goal to group core capabilities.

Mitigation: The capabilities necessary to reduce the loss of life and property from natural and/or manmade disasters by lessening the impacts of disasters.

Mobilization: The processes and procedures for activating, assembling, and transporting resources that have been requested to respond to or support an incident.

Multiagency Coordination Group: A group, typically consisting of agency administrators or executives from organizations, or their designees, that provides policy guidance to incident personnel, supports resource prioritization and allocation, and enables decision making among elected and appointed officials and senior executives in other organizations, as well as those directly responsible for incident management.

Multiagency Coordination System: An overarching term for the NIMS Command and Coordination systems: ICS, EOCs, MAC Group/policy groups, and JISs.

Mutual Aid Agreement or Assistance Agreement: A written or oral agreement between and among agencies/organizations and/or jurisdictions that provides a mechanism to quickly obtain assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate the rapid, short-term deployment of support prior to, during, and/or after an incident.

National: Of a nationwide character, including the local, state, tribal, territorial, and Federal aspects of governance and policy.

National Incident Management System: A systematic, proactive approach to guide all levels of government, NGOs, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from the effects of incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System. NIMS provides a consistent foundation for dealing with all incidents, ranging from daily occurrences to incidents requiring a coordinated Federal response.

National Planning Frameworks: Guidance documents for each of the five preparedness mission areas that describe how the whole community works together to achieve the National Preparedness Goal. The Frameworks foster a shared understanding of roles and responsibilities, from the firehouse to the White House, and clarifies how the Nation coordinates, shares information, and works together—ultimately resulting in a more secure and resilient Nation.

National Preparedness: The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation.

National Preparedness Goal: Doctrine describing what it means for the whole community to be prepared for the types of incidents that pose the greatest threat to the security of the Nation, including acts of terrorism and emergencies and disasters, regardless of cause. The goal itself is: "A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

National Preparedness System: An organized process to achieve the National Preparedness Goal of a secure and resilient Nation.

National Response Coordination Center: A multiagency coordination center located at FEMA Headquarters. Its staff coordinates the overall Federal support for major disasters and emergencies, including catastrophic incidents and emergency management program implementation.

Nongovernmental Organization: A group that is based on the interests of its members, individuals, or institutions. An NGO is not created by a government, but it may work cooperatively with government. Examples of NGOs include faith-based groups, relief agencies, organizations that support people with access and functional needs, and animal welfare organizations.

Normal Operations/Steady State: The activation level that describes routine monitoring of jurisdictional situation (no event or incident anticipated).

Officer: The ICS title for a member of the Command Staff authorized to make decisions and take action related to his/her area of responsibility.

Operational Period: The time scheduled for executing a given set of operation actions, as specified in the IAP. Operational periods can be of various lengths, but are typically 12 to 24 hours.

Operational Security: The implementation of procedures and activities to protect sensitive or classified operations involving sources and methods of intelligence collection, investigative techniques, tactical actions, countersurveillance measures, counterintelligence methods, undercover officers, cooperating witnesses, and informants.

Operations Section: The ICS Section responsible for implementing tactical incident operations described in the IAP. In ICS, the Operations Section may include subordinate branches, divisions, and/or groups.

Organization: Any association or group of persons with like objectives. Examples include, but are not limited to, governmental departments and agencies, NGOs, and private sector entities.

Plain Language: Communication that the intended audience can understand and that meets the communicator's purpose. For the purpose of NIMS, plain language refers to a communication style that avoids or limits the use of codes, abbreviations, and jargon, as appropriate, during incidents involving more than a single agency.

Planned Event (Event): An incident that is a scheduled non-emergency activity (e.g., sporting event, concert, parade).

Planning Meeting: A meeting held, as needed, before and throughout an incident to select specific strategies and tactics for incident control operations and for service and support planning.

Planning Section: The ICS Section that collects, evaluates, and disseminates 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.

Position Qualifications: The minimum criteria necessary for individuals to fill a specific position.

Prevention: The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. In national preparedness guidance, the term "prevention" refers to preventing imminent threats.

Private Sector: Organizations and individuals that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry.

Protection: The capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters.

Protocol: A set of established guidelines for actions (designated by individuals, teams, functions, or capabilities) under various specified conditions.

Public Information: Processes, procedures, and systems for communicating timely, accurate, and accessible information on an incident's cause, size, and current situation; resources committed; and other matters of general interest to the public, responders, and additional stakeholders (both directly affected and indirectly affected).

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

Recovery: The capabilities necessary to assist communities affected by an incident to recover effectively.

Recovery Plan: A plan to restore an incident-affected area or community.

Recovery Support Function: Organizing structures for key functional areas of assistance outlined in the National Disaster Recovery Framework that group capabilities of various government and private sector partner organizations to promote effective recovery from disasters before and after disasters strike.

Reimbursement: A mechanism to recoup funds expended for incident-specific activities.

Resource Management: Systems for identifying available resources at all jurisdictional levels to enable timely, efficient, and unimpeded access to resources needed to prepare for, respond to, or recover from an incident.

Resource Team: See *Strike Team.*

Resource Tracking: The process that all incident personnel and staff from associated organizations use to maintain information regarding the location and status of resources ordered for, deployed to, or assigned to an incident.

Resources: Personnel, equipment, teams, 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.

Response: The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

Safety Officer: In ICS, a member of the Command Staff responsible for monitoring incident operations and advising the Incident Commander or Unified Command on all matters relating to operational safety, including the health and safety of incident personnel. The Safety Officer modifies or stops the work of personnel to prevent unsafe acts.

Section: The ICS organizational element having responsibility for a major functional area of incident management (e.g., Operations, Planning, Logistics, and Finance/Administration).

Single Resource: An individual, a piece of equipment and its personnel complement, or a crew/team of individuals with an identified work supervisor that can be used on an incident.

Situation Report: Confirmed or verified information regarding the specific details relating to an incident.

Span of Control: The number of subordinates for which a supervisor is responsible, usually expressed as the ratio of supervisors to individuals.

Staging Area: A temporary location for available resources in which personnel, supplies, and equipment await operational assignment.

Standard Operating Procedure: A reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or several interrelated functions in a uniform manner.

State: Used in this document to include 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.

Status Report: Reports, such as spot reports, that include vital and/or time-sensitive information. Status reports are typically function-specific, less formal than situation reports, and are not always issued on a specific schedule.

Strategy: The general course of action or direction to accomplish incident objectives.

Strike Team: A set number of resources of the same kind and type that have an established minimum number of personnel, common communications, and a leader. In the law enforcement community, strike teams are referred to as resource teams.

Supervisor: The ICS title for an individual responsible for a division or group.

System: Any combination of processes, facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

Tactics: The deployment and directing of resources on an incident to accomplish the objectives.

Task Force: Any combination of resources of different kinds and/or types assembled to support a specific mission or operational need.

Terrorism: Any activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure and is a violation of the criminal laws of the United States or of any state or other subdivision of the United States; and appears to be intended to intimidate or coerce a civilian population, or to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat: A natural or manmade occurrence, an individual, an entity, or an action having or indicating the potential to harm life, information, operations, the environment, and/or property.

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

Type: A NIMS resource classification that refers to capability of a specific kind of resource to which a metric is applied to designate it as a specific numbered class.

Unified Area Command: A version of command established when incidents under an Area Command are multijurisdictional. See *Area Command*.

Unified Command: An ICS application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions.

Unit: The organizational element with functional responsibility for a specific activity within the Planning, Logistics, and Finance/Administration Sections in ICS.

Unit Leader: The individual in charge of a unit in ICS.

United States National Grid: A point and area location reference system that FEMA and other incident management organizations use as an accurate and expeditious alternative to latitude/longitude.

Unity of Command: A NIMS guiding principle stating that each individual involved in incident management reports to and takes direction from only one person.

Unity of Effort: A NIMS guiding principle that provides coordination through cooperation and common interests and does not interfere with Federal department and agency supervisory, command, or statutory authorities.

Whole Community: A focus on enabling the participation in incident management activities of a wide range of players from the private and nonprofit sectors, including NGOs and the general public, in conjunction with the participation of all levels of government, to foster better coordination and working relationships.

VII. List of Abbreviations

AHJ	Authority Having Jurisdiction
ANSI	American National Standards Institute
CFR	Code of Federal Regulations
CPG	Comprehensive Preparedness Guide
DHS	Department of Homeland Security
DOC	Departmental Operations Center
EAS	Emergency Alert System
EEI	Essential Elements of Information
EMAC	Emergency Management Assistance Compact
EMS	Emergency Medical Services
EOC	Emergency Operations Center
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIRESCOPE	Firefighting Resources of California Organized for Potential Emergencies
GIS	Geographic/Geospatial Information Systems
HazMat	Hazardous Material
HHS	Health and Human Services
IAP	Incident Action Plan
ICP	Incident Command Post
ICS	Incident Command System
IMAT	Incident Management Assistance Team
IMT	Incident Management Team
IPAWS	Integrated Public Alert and Warning System
IRIS	Incident Resource Inventory System
ISM	Incident Support Model

IT	Information Technology
JFO	Joint Field Office
JIC	Joint Information Center
JIS	Joint Information System
MAC Group	Multiagency Coordination Group
MACS	Multiagency Coordination System
NECP	National Emergency Communications Plan
NFPA	National Fire Protection Association
NGO	Nongovernmental Organization
NIEM	National Information Exchange Model
NIIMS	National Interagency Incident Management System
NIMS	National Incident Management System
NRCC	National Response Coordination Center
NTAS	National Terrorism Advisory System
NWCG	National Wildfire Coordinating Group
PETS Act	Pet Evacuation and Transportation Standards Act of 2006
PIO	Public Information Officer
PKEMRA	Post-Katrina Emergency Management Reform Act of 2006
PTB	Position Task Book
Pub. L.	Public Law
RSF	Recovery Support Function
RTLT	Resource Typing Library Tool
SITREP	Situation Report
SOP	Standard Operating Procedure
THIRA	Threat and Hazard Identification and Risk Assessment
USCG	United States Coast Guard

VIII. Resources

A. NIMS Supporting Documents

FEMA has developed, or is developing, a variety of documents and resources to support NIMS implementation. The hub for all information is http://www.fema.gov/national-incident-management-system.

Guidelines for the Credentialing of Personnel

- The NIMS Guideline for the Credentialing of Personnel describes the national credentialing standards and provides written guidance regarding the use of those standards. This document describes credentialing and typing processes and identifies tools that emergency management personnel at all levels of government use, both routinely and to facilitate multijurisdictional coordinated responses.
- https://www.fema.gov/resource-management-mutual-aid

ICS Forms Booklet

- The NIMS ICS Forms Booklet, FEMA 502-2, assists emergency response personnel in the use of ICS and corresponding documentation during incident operations.
- https://www.fema.gov/incident-command-system-resources

NIMS Intelligence and Investigations Function Guidance and Field Operations Guide

- This document includes guidance on how various disciplines can use and integrate the intelligence/investigations function while adhering to NIMS concepts and principles. It includes information intended for the NIMS practitioner (including the Incident Commander or Unified Command) that assists in the placement of the intelligence/investigations function within the command structure; provides guidance for implementing the intelligence/investigations function; and has an accompanying Intelligence and Investigations Function Guidance and Field Operations Guide.
- https://www.fema.gov/nims-doctrine-supporting-guides-tools

NIMS Resource Center

- The FEMA NIMS website contains links to a number of supporting guides and tools for NIMS implementation. As FEMA develops new items, they will be added to this website.
- https://www.fema.gov/national-incident-management-system

NIMS Training Program

- Supersedes the previous training guidance, the Five-Year NIMS Training Program.

- The NIMS Training Program specifies FEMA and stakeholder responsibilities and activities for developing, maintaining, and sustaining NIMS training. The NIMS Training Program outlines responsibilities and activities that are consistent with the National Training Program, as mandated by the Post-Katrina Emergency Management Reform Act (PKEMRA) of 2006.
- https://www.fema.gov/training-0

B. Relevant Law

Homeland Security Act of 2002

- The Homeland Security Act of 2002, Pub. L. 107-296, enacted November 25, 2002, establishes DHS.
- http://www.dhs.gov/homeland-security-act-2002

Pet Evacuation and Transportation Standards Act (PETS Act) of 2006

- The PETS Act of 2006 amends the Robert T. Stafford Disaster Relief and Emergency Assistance Act to require the FEMA Administrator to ensure that state and local emergency preparedness operational plans address the needs of individuals with household pets and service animals prior to, during, and following a major disaster or emergency and authorizes Federal agencies to provide, as assistance essential to meeting threats to life and property resulting from a major disaster, rescue, care, shelter, and essential needs to individuals with household pets and service animals and to such pets and animals.
- https://www.gpo.gov/fdsys/pkg/PLAW-109publ308/pdf/PLAW-109publ308.pdf

Post-Katrina Emergency Management Reform Act (PKEMRA) of 2006

- PKEMRA amends the Homeland Security Act of 2002 to make extensive revisions to emergency response provisions while keeping FEMA within DHS. PKEMRA significantly reorganizes FEMA, providing it substantial new authority to remedy gaps in response, and includes a more robust preparedness mission for FEMA.
- https://www.gpo.gov/fdsys/pkg/PLAW-109publ295/pdf/PLAW-109publ295.pdf

Robert T. Stafford Disaster Relief and Emergency Assistance Act

- Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law (Pub. L.) 100-707, signed into law November 23, 1988; amends the Disaster Relief Act of 1974, Pub. L. 93-288. This Act constitutes the statutory authority for most Federal disaster response activities, especially as they pertain to FEMA and FEMA programs.
- http://www.fema.gov/robert-t-stafford-disaster-relief-and-emergency-assistance-act-public-law-93-288-amended

Sandy Recovery Improvement Act of 2013

- The Sandy Recovery Improvement Act of 2013 became law on January 29, 2013, and amends the Robert T. Stafford Disaster Relief and Emergency Assistance Act. This Act

authorizes changes to the way FEMA delivers Federal disaster assistance with the goals of (1) reducing the costs to the Federal Government of providing such assistance; (2) increasing flexibility in the administration of assistance; (3) expediting the provision of assistance to a state, tribal, or local government, or owner or operator of a private nonprofit facility; and (4) providing financial incentives and disincentives for the timely and cost-effective completion of projects.

- https://www.congress.gov/113/bills/hr219/BILLS-113hr219rds.pdf

C. Additional Supporting Materials

Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans, Version 2

- Published in November 2010, FEMA's CPG 101, Version 2.0 provides guidance on the fundamentals of planning and development of emergency operations plans. CPG 101, Version 2.0 encourages emergency and homeland security managers to engage the whole community in addressing the risks that potentially impact their jurisdictions.

- http://www.fema.gov/plan

CPG 201, Threat and Hazard Identification and Risk Assessment Guide, Second Edition

- Published in August 2013, CPG 201, Second Edition, provides communities guidance for conducting a Threat and Hazard Identification and Risk Assessment (THIRA). This guide describes a standard process for identifying community-specific threats and hazards, setting capability targets for each core capability identified in the National Preparedness Goal, and estimating resource requirements.

- http://www.fema.gov/threat-and-hazard-identification-and-risk-assessment

Emergency Management Assistance Compact (EMAC)

- EMAC became law in 1996 (Pub. L. 104-321) and offers assistance during governor-declared states of emergency through a responsive, straightforward system that allows states to send personnel, equipment, and commodities to help disaster relief efforts in other states. Through EMAC, states can also transfer services, such as shipping diagnostic specimens from a disaster-impacted lab to a lab in another state.

- http://www.emacweb.org/

Incident Resource Inventory System (IRIS)

- IRIS is a distributed software tool provided by FEMA. All agencies, jurisdictions, and communities can use IRIS as a consistent tool to inventory resources into their own database and to search/identify their specific resources for incident operations and mutual aid purposes.

- https://www.fema.gov/resource-management-mutual-aid

National Emergency Communications Plan (NECP)

- The NECP is the Nation's strategic plan for emergency communications that promotes communication and sharing of information across all levels of government, jurisdictions, disciplines, and organizations for all threats and hazards, as needed and when authorized.
- https://www.dhs.gov/national-emergency-communications-plan

National Information Exchange Model (NIEM)

- NIEM is a community-driven, standards-based approach to exchanging information. Diverse communities can collectively use NIEM to increase efficiencies and improve decision making.
- https://www.niem.gov

National Planning Frameworks

- The National Planning Frameworks, one for each mission area, describe how the whole community works together to achieve the National Preparedness Goal.
- http://www.fema.gov/national-planning-frameworks

National Preparedness Goal

- The National Preparedness Goal defines what it means for the whole community to be prepared for all types of disasters and emergencies. The goal itself is succinct: "A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."
- http://www.fema.gov/national-preparedness-goal

National Preparedness System

- The National Preparedness System outlines an organized process for everyone in the whole community to move forward with their preparedness activities and achieve the National Preparedness Goal.
- http://www.fema.gov/national-preparedness-system

National Wildfire Coordinating Group (NWCG)

- The NWCG provides national leadership to develop, maintain, and communicate interagency standards, guidelines, qualifications, training, and other capabilities that enable interoperable operations among Federal and non-Federal entities. NWCG standards are interagency by design. The individual member entities independently decide whether to adopt and use them, and communicate them through their respective directives systems.
- http://www.nwcg.gov/

Resource Management and Mutual Aid Guidance

- Resource Management guidance and tools support the use of consistent resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.
- https://www.fema.gov/resource-management-mutual-aid

Resource Typing Library Tool (RTLT)

- The RTLT is an online catalog of national resource typing definitions and job titles/position qualifications. Definitions and job titles/position qualifications are easily searchable and discoverable through the RTLT.
- https://www.fema.gov/resource-management-mutual-aid

United States Coast Guard (USCG)

- The Coast Guard uses NIMS guidance extensively and has expertise in the application of the elements of NIMS. USCG efforts have helped to extend the audience for NIMS by institutionalizing the use of ICS for incidents involving spills and security operations.
- http://www.uscg.mil/

Using Social Media for Enhanced Situational Awareness and Decision Support

- Published in June 2014, the report "Using Social Media for Enhanced Situational Awareness and Decision Support" provides examples of how organizations use social media to enhance situational awareness and support operational decision making, as well as challenges and potential applications.
- https://www.dhs.gov/publication/using-social-media-enhanced-situational-awareness-decision-support

Appendix A. Incident Command System

A. Purpose

This appendix provides additional explanation and examples of the Incident Command System (ICS), but it is not ICS training.

ICS is used for a broad spectrum of incidents (routine to complex, naturally occurring and human-caused) and by all levels of government (local, state, tribal, territorial, insular area, and Federal) as well as nongovernmental organizations (NGO) and the private sector. ICS combines facilities, equipment, personnel, procedures, and communications involved with on-scene incident management activities.

The important steps in applying ICS to an incident are:

- Establishing and transferring command as appropriate;
- Identifying and activating the organizational elements that are needed;
- Delegating authority as appropriate;
- Establishing incident facilities as needed to support field operations;
- Using ICS common terminology in establishing organizational elements, position titles, facilities, and resources; and
- Determining incident objectives and initiating the incident action planning process; transitioning from oral plans to written Incident Action Plans (IAP).

B. Organization of This Appendix

The major elements of ICS are organized into the following ten tabs:

- Tab 1—ICS Organization
- Tab 2—The Operations Section
- Tab 3—The Planning Section
- Tab 4—The Logistics Section
- Tab 5—The Finance/Administration Section
- Tab 6—The Intelligence/Investigations Function
- Tab 7—Consolidating the Management of Multiple Incidents

- Tab 8—Incident Action Planning
- Tab 9—ICS Forms
- Tab 10—Primary Functions of Incident Commander or Unified Command, Command Staff, and General Staff Positions

ICS Tab 1—ICS Organization

Functional Structure

ICS consists of five major functional areas, staffed as needed. They are Command, Operations, Planning, Logistics, and Finance/Administration.

Modular Expansion

The ICS organizational structure is modular, expanding to incorporate all elements necessary for the type, size, scope, and complexity of an incident. The ICS structure builds from the top down; responsibility and performance begin with incident command. If one individual can simultaneously manage all major functional areas, no further organization is needed. If one or more of the functions needs independent management, an individual is assigned responsibility for that function.

The initial Incident Commander determines which Command or General Staff positions to staff in order to maintain a manageable span of control and ensure appropriate attention to the necessary incident management functions. An Incident Commander activates Command Staff officers (e.g., Public Information Officer [PIO], Safety Officer, and Liaison Officer) and four section chiefs (Operations, Planning, Logistics, and Finance/Administration) as needed. Personnel in these positions further delegate management authority for their areas as necessary. The Command Staff may assign assistants, and section chiefs may assign deputies and assistants and may establish branches, groups, divisions, or units, depending on the section.

Modular expansion at an incident is based on the following considerations:

- Developing the organization's structure to match the function or task to be performed;
- Staffing only the organizational elements needed to perform the task;
- Ensuring manageable span of control;
- Performing the function of any non-activated organizational element at the next higher level; and
- Demobilizing organizational elements no longer needed.

The use of deputies and assistants is a vital part of both the organizational structure and the modular concept. The Incident Commander may have one or more deputies who may be from the same or an assisting jurisdiction/organization. The primary reasons to designate a Deputy Incident Commander are:

- To perform specific tasks as the Incident Commander directs;
- To perform the command function in a relief capacity (e.g., to take over the next operational period; in this case, the deputy then assumes the primary role); and
- To represent an assisting agency that may share jurisdiction or have jurisdiction in the future.

Deputies are used at section and branch levels of the incident organization. A deputy, whether at the command, section, or branch level, is qualified to assume the position.

Assistants are used on Command Staffs and to support section chiefs. Unlike deputies, assistants have a level of technical capability, qualification, and responsibility subordinate to the primary positions and need not be fully qualified to assume the position.

For reference, Table A-1 describes the distinctive title or titles assigned to each element of the ICS organization, as well as the titles of corresponding leadership and support positions.

Table A-1: ICS Organization

Organizational Element	Leadership Position Title	Support Positions
Incident Command	Incident Commander	Deputy
Command Staff	Officer	Assistant
Section	Chief	Deputy, Assistant
Branch	Director	Deputy
Divisions/Groups	Supervisors	N/A
Unit	Unit Leader	Manager, Coordinator
Strike Team/Task Force	Leader	Single Resource Boss
Single Resource	Boss, Leader	N/A
Technical Specialist	Specialist	N/A

Command Staff

In an ICS organization, incident command consists of the Incident Commander and various Command Staff positions. The Command Staff are specifically designated, report directly to the Incident Commander, and are assigned responsibility for key activities that are not a part of the General Staff functional elements. Three Command Staff positions are typically identified in ICS: PIO, Safety Officer, and Liaison Officer. The Incident Commander may assign technical specialists as additional command advisors, depending on the nature, scope, complexity, and location(s) of the incident(s), or according to specific needs the Incident Commander or Unified Command establishes.

Public Information Officer

The PIO is responsible for interfacing with the public, the media, and with other jurisdictions/organizations with incident-related information needs. The PIO gathers, verifies, coordinates, and disseminates accurate, accessible, and timely information regarding the incident. The Incident Commander or Unified Command approves the release of incident-related information. The PIO serves as the primary on-scene connection to other ongoing Joint Information System (JIS) activities and participates in or leads the Joint Information Center (JIC) to ensure consistency of information provided to the public. The PIO also monitors the media and other sources of public information to collect relevant information and transmits this

information to the appropriate personnel at the incident, a supporting Emergency Operations Center (EOC), and/or a Multiagency Coordination Group (MAC Group).

The PIO performs a key public information-monitoring role by implementing measures for rumor control and monitoring/updating incident-related social media posts.

A lead PIO is designated, regardless of whether the command structure is single or unified. The PIO may have assistants, as necessary, which other agencies, departments, or organizations involved in the incident may assign.

Safety Officer

The Safety Officer monitors incident operations and advises the Incident Commander or Unified Command on all matters relating to operational safety, including the health and safety of incident personnel. Ultimately, responsibility for conducting incident management operations safely rests with the Incident Commander or Unified Command and supervisory personnel at all levels of incident management. The Safety Officer, in turn, is responsible to the Incident Commander or Unified Command for the systems and procedures necessary to ensure the ongoing assessment of hazardous environments, including development of the incident Safety Plan, coordination of multiagency safety efforts, and implementation of measures to promote incident personnel safety, as well as the general safety of incident operations. To carry out these responsibilities, the Safety Officer alters, suspends, or terminates any activities that are immediately dangerous to life and health of personnel.

In a Unified Command structure, a single Safety Officer[20] is designated regardless of the involvement of multiple jurisdictions or organizations. The Safety Officer coordinates closely with all section chiefs regarding operational safety and emergency responder health and safety issues. The Safety Officer ensures the coordination of safety management functions and issues across jurisdictions, across functional agencies, and with NGOs and the private sector. 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 personnel involved in incident operations.

For more complex incidents, the Safety Officer may designate one or more Assistant Safety Officers to perform specific tasks and/or manage day-to-day functions on a more complex incident or to represent an assisting agency that may share jurisdiction or have jurisdiction in the future. The Safety Officer may also designate assistants to bring specific skill sets or expertise relevant to the incident. The following examples describe Assistant Safety Officers that a Safety Officer might request:

- An Assistant Safety Officer for hazardous material (HazMat) to carry out the functions outlined in 29 CFR 1910.120 (Hazardous Waste Operations and Emergency Response).
- An Assistant Safety Officer for Fire to oversee fire suppression operations.

[20] Resources, such as Urban Search and Rescue teams, may include their own Safety Officers; such Safety Officers retain their specific responsibilities and authorities and coordinate with the Safety Officer on the Command Staff as necessary.

- An Assistant Safety Officer for Food to oversee food handling and distribution.

Figure A-1 depicts Assistant Safety Officers for HazMat, Fire, and Food organizationally positioned in an incident. Assistant Safety Officers may also be assigned to divisions or groups in the field.

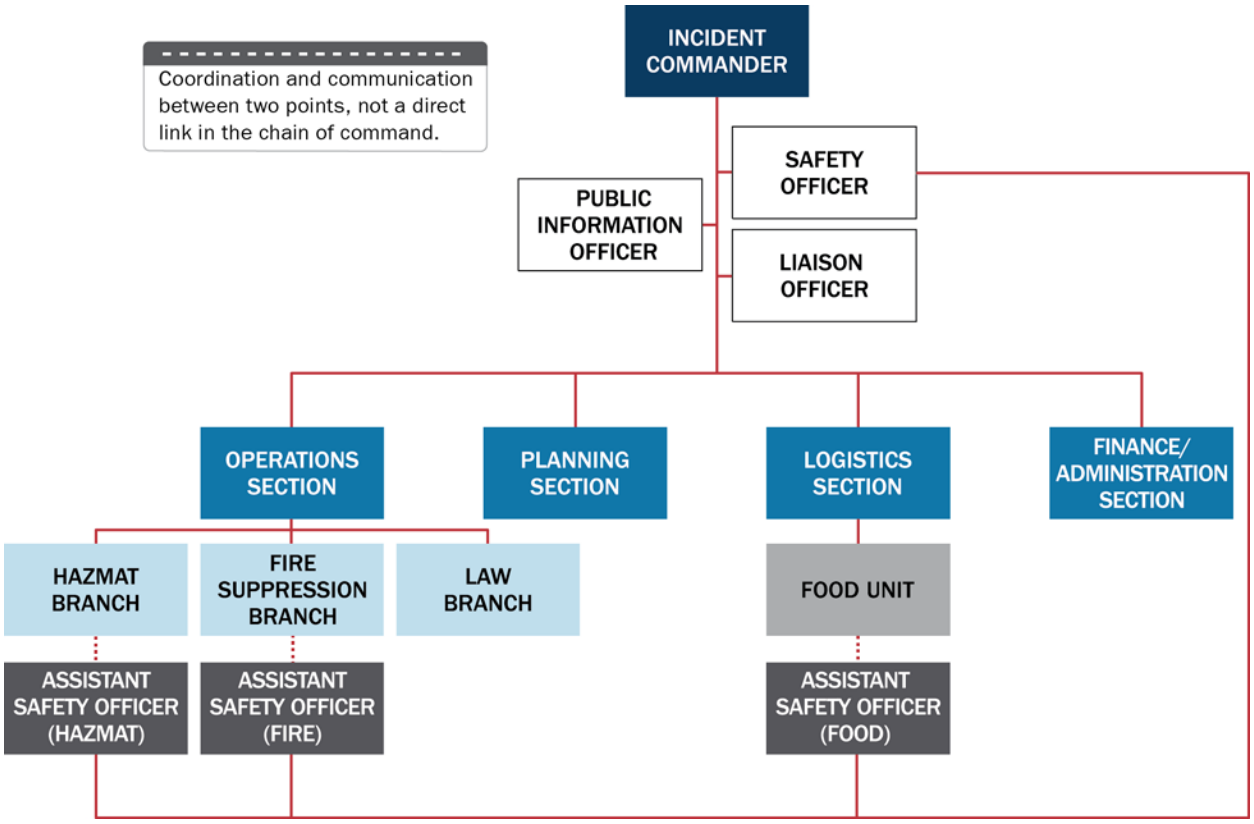


Figure A-1: Example of Assistant Safety Officers in ICS in an Incident with Multiple Branches

Liaison Officer

The Liaison Officer is a conduit of information and assistance between incident personnel and organizations that are assisting or cooperating with the response. Through the Liaison Officer, agencies lacking jurisdiction or legal authority for the management of the incident—such as other governmental organizations, NGOs, and private sector organizations—provide input regarding their policies, resource availability, and other incident-related matters. These organizations appoint Agency Representatives, who coordinate directly with the Liaison Officer.

Whether a single Incident Commander or Unified Command structure is in place, representatives from assisting or cooperating agencies coordinate through the Liaison Officer. Agency Representatives assigned to an incident speak for their parent agencies or organizations. Personnel from other agencies or organizations—public or private—involved in incident management activities are assigned to the Liaison Officer to facilitate coordination.

For more complex incidents, the Liaison Officer may have one or more assistants, who may be from the same or an assisting agency.

Command Advisors

In addition to the three Command Staff officer positions, the Incident Commander or Unified Command may choose to appoint technical specialists as command advisors. For example, the Incident Commander or Unified Command may appoint:

- A legal counsel to advise on legal matters such as those related to emergency declarations, evacuation and quarantine orders, and rights and restrictions pertaining to media access;
- A Medical Advisor to provide guidance and recommendations to incident command regarding a broad range of areas such as medical care, acute care, long-term care, behavioral services, mass casualties, vector control, epidemiology, or mass prophylaxis;
- A Science and Technology Advisor to monitor incident operations and advise incident command on the integration of science and technology into planning and decision making; and
- An Access and Functional Needs Advisor to provide expertise regarding communication, transportation, supervision, and essential services for diverse populations in the affected area.

Technical specialists may be assigned anywhere in the organization and are described in this appendix under ICS Tab 3.

ICS Tab 2—The Operations Section

Operations Section staff are responsible for tactical activities that typically focus on saving lives, reducing the immediate hazard, protecting property and the environment, establishing situational control, and restoring normal operations. Lifesaving and responder safety are always the highest priorities.

The responsibility and composition of the Operations Section change according to incident type and complexity. Organizations that may work together in the Operations Section include fire, law enforcement, public health, public works, emergency medical services (EMS), NGOs, and the private sector. Depending on the situation, these organizations may be organized in branches, divisions, groups, task forces, and/or strike teams.

Figure A-2 depicts the organizational template for an Operations Section, though the structure's configuration on any given incident varies according to the incident's needs, the jurisdictions/organizations involved, and the objectives and tactics of the incident management effort. The following discussion presents several different methods of organizing tactical operations on an incident.

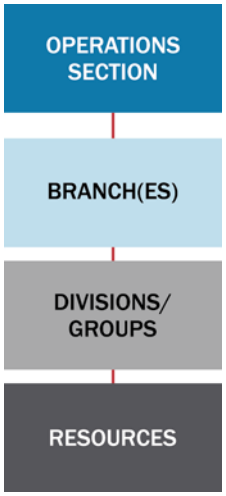


Figure A-2: Major Organizational Elements of the Operations Section

Operations Section Chief

The Operations Section Chief manages tactical incident activities and oversees implementation of the IAP. The Operations Section Chief may have one or more deputies and/or assistants. The Operations Section Chief for each operational period has direct responsibilities for IAP development for the next operational period.

The Operations Section Chief may organize Operations Section staff in various ways to meet different challenges. In some cases, a strictly functional approach is used. In other cases, geographic or jurisdictional boundaries determine the organizational structure. In still others, a mix of functional and geographic considerations is appropriate. ICS offers flexibility in determining the right structural approach for the specific circumstances of the incident at hand.

Maintaining Manageable Span of Control for the Operations Section

The Operations Section Chief organizes the section and assigns subordinate supervisory personnel as necessary to maintain a manageable span of control. Different options for organizing the Operations Section are below.

Branches

Branches are inserted between the Operations Section Chief and divisions and/or groups, as described below, when the number of divisions and/or groups exceeds a manageable span of control.

Geographic Branch Structure

The Operations Section Chief establishes geographic branches to maintain a manageable span of control in the Operations Section by grouping two or more divisions and/or groups. The boundaries of geographic branches are thus defined by the combined areas of the divisions that comprise each branch. For example, if four divisions are reporting to the Operations Section Chief and an additional two divisions are needed, and all need close oversight, a two-branch organization is formed (see Figure A-3).

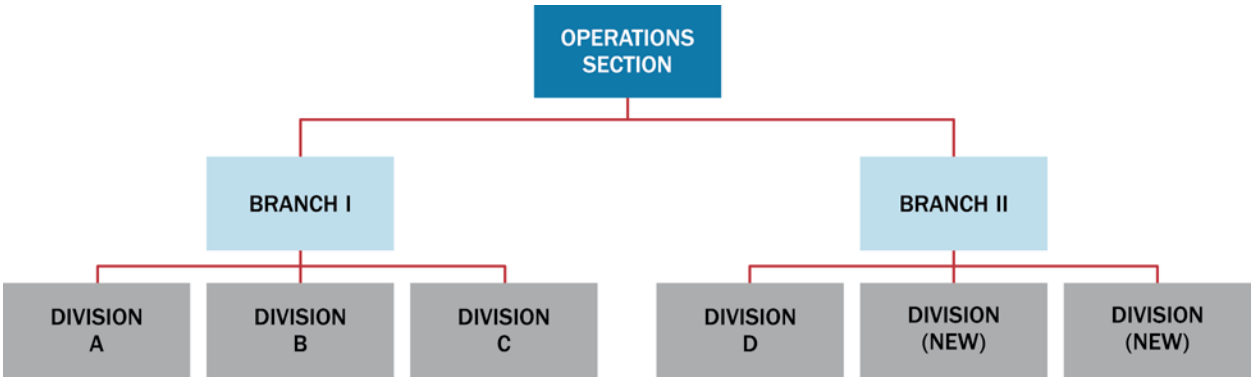


Figure A-3: Geographic Branch Organization

Geographic branch boundaries are depicted on incident maps and clearly communicated to incident personnel.

Functional Branch Structure

The following example illustrates a functional branch structure: If a large aircraft crashes in a local jurisdiction, various disciplines (including law enforcement, fire, EMS, public works, and public health) may each have a functional branch operating under a single Operations Section Chief's direction. In this example (shown in Figure A-4), the Operations Section Chief is from the fire department with deputies from law enforcement and EMS. The Operations Section Chief may organize around different functional groups, depending on the jurisdiction's plan and the incident type.

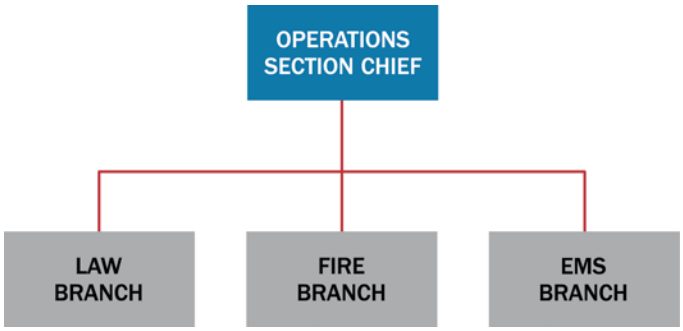


Figure A-4: A Functional Branch Structure

Divisions and Groups

The Operations Section Chief establishes divisions and groups when the number of resources exceeds his or her manageable span of control. Divisions always refer to geographic assignments and groups always refer to functional assignments. Both divisions and groups may be used in a single incident. Maintaining proper coordination is vital to the success of these operations.

Divisions

Divisions separate physical or geographic areas of operation within the incident area. Divisions can be established according to political or natural terrain boundaries or other prominent geographic features, such as rivers, major roadways, or floors in a multistory building response. As with branch boundaries, division boundaries are depicted on incident maps and communicated to incident personnel (see Figure A-5).

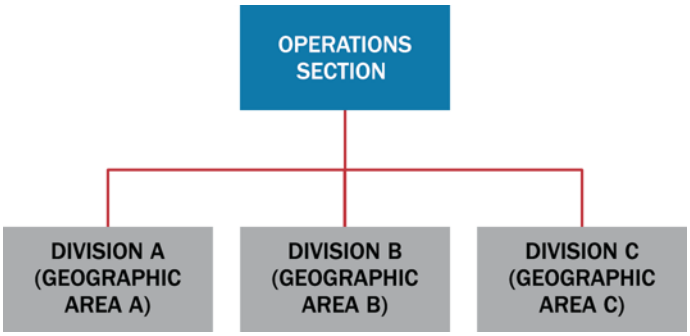


Figure A-5: Use of Geographical Divisions

Functional Groups

Groups are used to describe functional areas of similar activity (e.g., rescue, evacuation, law enforcement, or medical treatment or triage), as shown in Figure A-6.

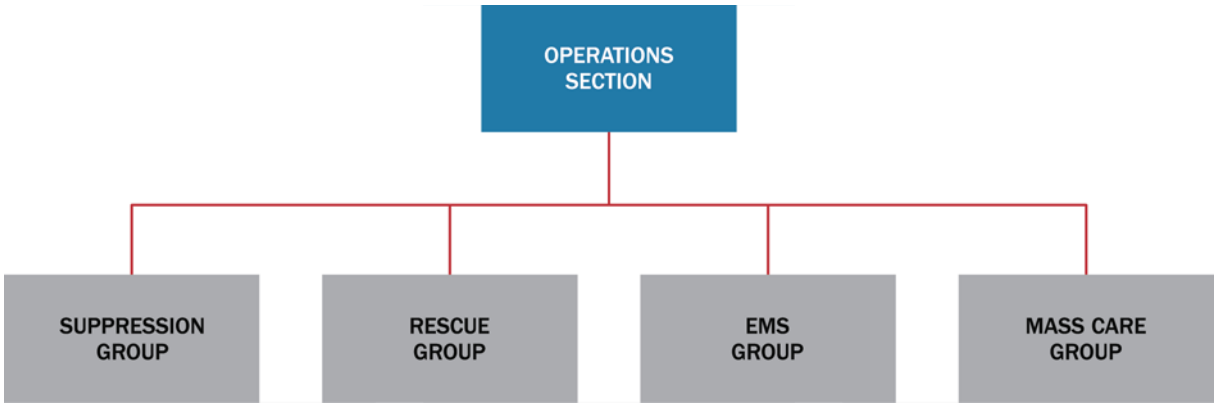


Figure A-6: Use of Functional Groups

Combined Geographic Divisions and Functional Groups

It is possible to have both divisions and groups within the Operations Section. Supervisors of divisions and groups have the same level of authority. For example, Divisions A, B, and C (based on geographic locations) may work in conjunction with functional groups assigned to specific tasks (e.g., traffic control and smoke ventilation) in those locations. Alternatively, groups may be assigned throughout the incident and may work independently or in conjunction with divisions.

Organizing Resources

Consolidating single resources into task forces and strike teams reduces supervisors' spans of control. As the incident grows in size and complexity, task forces and strike teams are typically organized into divisions and/or groups.

Single Resources

Resources may be employed on a single basis, such as an individual person or an individual piece of equipment with its associated operators.

Task Forces

Task forces combine different kinds and types of resources to accomplish a specific mission under a designated leader. They enable one supervisor to manage several key resource elements. As an example, during a flood, a public works task force may be established to open storm drains. The task force may consist of a dump truck, a backhoe, a five-person crew with shovels and transportation, and a task force leader (e.g., public works supervisor).

Strike Teams

Strike teams are another means of combining resources. Strike teams consist of a set number of resources of the same kind and type operating under a designated leader. As an example, a Debris Removal Strike Team could consist of five Type 3 dump trucks and a Strike Team Leader. In the law enforcement community, strike teams are known as resource teams.

Air Operations Branch

When a single helicopter is the only air asset on an incident, it is usually under the Operations Section Chief's direct control. When the complexity of air operations involves additional support and/or air-space control (including mixing tactical and support use of helicopters and other aircraft), the Operations Section Chief establishes an Air Operations Branch. An Air Operations Branch helps ensure the safe and efficient use of aviation resources. Figure A-7 shows a typical organizational structure for air operations.

When helicopters and fixed-wing aircraft operate simultaneously within the incident airspace, the Operations Section Chief designates an Air Tactical Group Supervisor. This individual coordinates all air activity with the assistance of a Helicopter Coordinator and a Fixed-Wing Coordinator.

Air Support Group staff establish and operate bases for helicopters and maintain a liaison with off-incident fixed-wing bases. Staff in the Air Support Group are responsible for all timekeeping for aviation resources assigned to the incident.

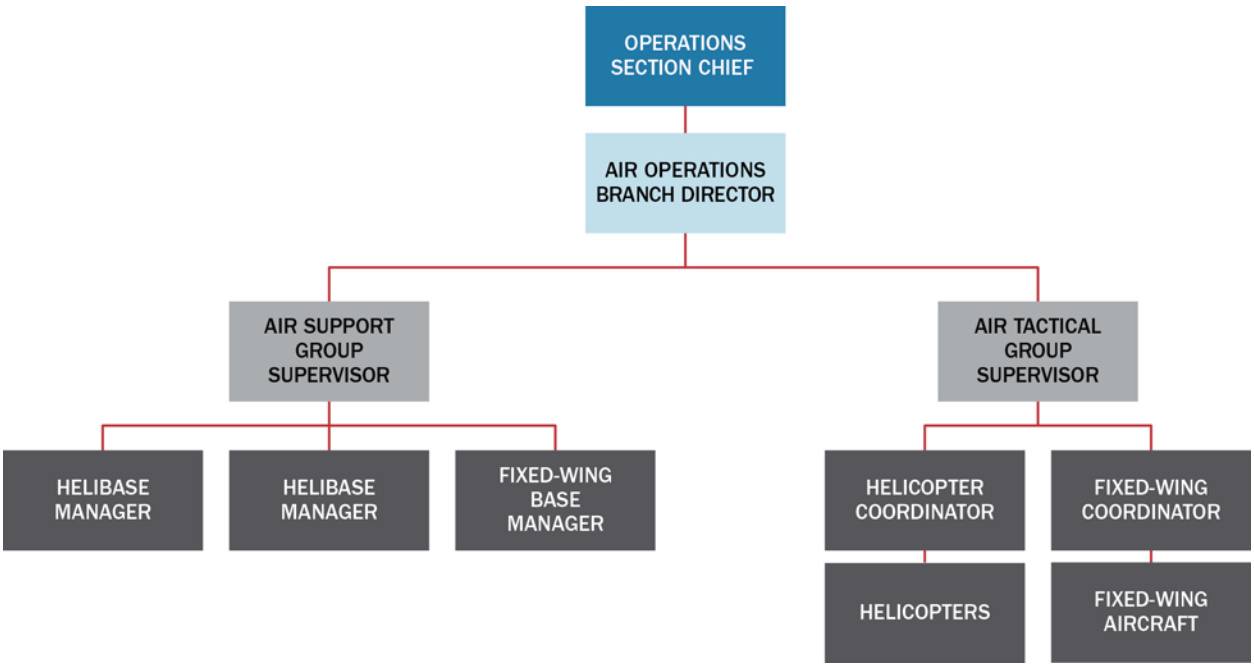


Figure A-7: Air Operations Organization

ICS Tab 3—The Planning Section

Staff in the Planning Section collect, evaluate, and disseminate operational information pertaining to the incident. Staff in this section maintain information on the current and forecasted situation as well as the status of resources assigned to the incident. Planning Section staff prepare IAPs and incident maps and gather and disseminate information important to the incident.

The Planning Section Chief leads the Planning Section, which has four primary units (as shown in Figure A-8). The Planning Section may also include technical specialists who typically provide expertise in specific areas and assist in evaluating the situation and forecasting needs for additional personnel and equipment.

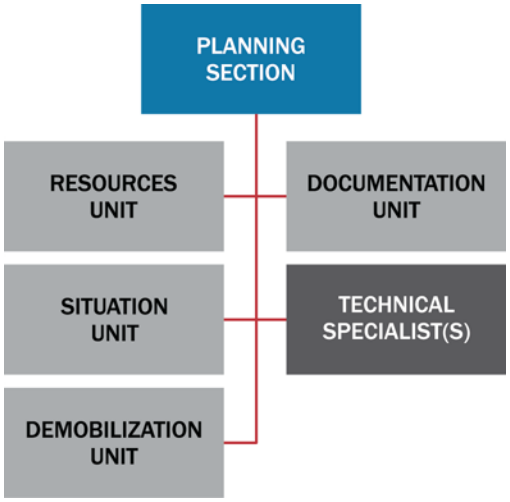


Figure A-8: Planning Section Organization

Planning Section Chief

The Planning Section Chief oversees incident-related data gathering and analysis regarding incident operations and assigned resources, facilitates incident action planning meetings, and prepares the IAP for each operational period. This individual normally comes from the jurisdiction or organization with primary incident responsibility and may have one or more deputies who may come from other participating jurisdictions or organizations.

Resources Unit

Responsibilities

Resources Unit staff track the location and status of all resources assigned to an incident. They ensure all assigned resources have checked in at the incident.

Resource Status

Staff in the Resources Unit track resource status continuously to manage resources effectively during an incident. They use the following status conditions for maintaining an up-to-date and accurate picture of resource status:

- ***Assigned***: Resources that have been checked in and assigned work tasks on an incident.

- ***Available***: Resources assigned to an incident, checked in, and available for a mission assignment, normally located in a staging area.
- ***Out of Service***: Resources that are checked in, but are not assigned and not available for assignment for mechanical, rest, or personnel reasons.

Resource Tracking

The Resources Unit tracks resources assigned to an incident, but Logistics Section staff track resources that have been ordered but have not yet arrived at the incident.

When a resource's status changes (e.g., a unit that was previously "out of service" is now "available"), the Unit Leader or the supervisor who approved the status change immediately notifies the Resources Unit Leader, who documents the status change.

Situation Unit

Situation Unit staff collect, process, and organize situation information, prepare situation summaries, and develop projections and forecasts related to the incident. They gather and disseminate information for the IAP. This unit produces Situation Reports (SITREP) as scheduled or at the request of the Planning Section Chief or Incident Commander. The Situation Unit frequently includes Geographic/Geospatial Information Systems (GIS) Specialists, who produce maps, and other technical specialists. The Situation Unit may also include Field Observers to gather information on the incident and/or response.

Documentation Unit

Documentation Unit staff maintain incident files and data for legal, analytical, and historical purposes, including a complete record of the major steps taken to resolve the incident. They also provide duplication services for incident personnel; compile, reproduce, and distribute the IAP; and maintain the files and records that are developed as part of the IAP and planning function.

Demobilization Unit

Demobilization Unit staff develop an Incident Demobilization Plan that includes specific instructions for all personnel and other resources to be demobilized. They begin their work early in the incident, creating rosters of personnel and resources and obtaining any missing information as check-in proceeds. Once the Incident Commander or Unified Command has approved the Incident Demobilization Plan, Demobilization Unit staff ensure its distribution at the incident and elsewhere, as necessary. For major incidents, demobilization plans are dynamic and the staff in the Demobilization Unit may need to update them frequently.

Technical Specialists

ICS functions in a wide variety of incidents that need technical specialists. Technical specialists have special expertise and skills, and they are activated only when needed. No specific 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 certified in their fields or professions.

Technical specialists may serve anywhere within the organization depending on factors such as complexity, span of control, lines of communication, and subject matter expertise. They are most often assigned to the specific area (section, branch, division, group, or unit) where their services are needed. Technical specialists assigned to the Command Staff are called command advisors. In some situations, they are assigned to a separate unit within the Planning Section, much like a talent pool, and assigned out to various jobs on a temporary basis.

Generally, if the expertise is needed for only a short time and involves only one individual, that individual is assigned to the Situation Unit. If the expertise is needed on a long-term basis and necessitates several persons, a separate Technical Unit is established in the Planning Section.

Examples of Technical Specialists

- Access and functional needs advisor
- Agricultural specialist
- Community representative
- Decontamination specialist
- Environmental impact specialist
- Epidemiologist
- Flood control specialist
- Health physicist
- Industrial hygienist
- Intelligence specialist
- Legal advisor
- Behavioral health specialist
- Meteorologist
- Science and technology advisor
- Pharmacist
- Veterinarian
- Toxicologist

ICS Tab 4—The Logistics Section

Logistics Section staff provide for all the incident's support needs, such as ordering resources and providing facilities, transportation, supplies, equipment maintenance and fuel, communications, and food and medical services for incident personnel.

The Logistics Section Chief leads the Logistics Section, sometimes with one or more deputies and/or assistants. When the incident is very large or needs several facilities and/or large quantities of equipment, the Logistics Section Chief may divide the Logistics Section into branches. This helps maintain a manageable span of control by providing more effective supervision and coordination among the units.

Figure A-9 provides an example of the Logistics Section organized with Service and Support Branches.

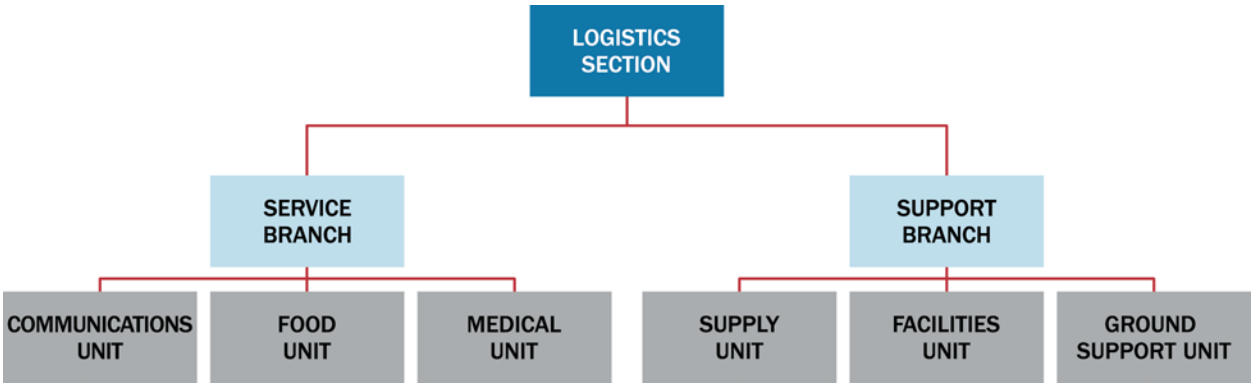


Figure A-9: Logistics Section with Branch Organizational Structure

Logistics Section Chief

The Logistics Section Chief is responsible for providing facilities, services, people, and material for the incident. The Logistics Section Chief participates in the IAP's development and supervises the Logistics Section's branches or units.

Supply Unit

Supply Unit staff order, receive, process, store, inventory, and distribute all incident-related resources.

The Supply Unit staff are responsible for all off-incident ordering, including obtaining the following:

- Tactical and support resources (including personnel); and
- Expendable and nonexpendable supplies.

The Supply Unit staff provide support to receive, process, store, and distribute all supply orders. They handle tool operations, which includes storing, distributing, and servicing tools and portable, nonexpendable equipment. Additionally, the Supply Unit staff assist in projecting resource needs.

Facilities Unit

Facilities Unit staff set up, maintain, and demobilize all facilities used in support of incident operations. This staff provides facility maintenance and law enforcement/security services needed for incident support.

Facilities Unit staff set up the Incident Command Post (ICP), Incident Base, and camps (including trailers or other forms of shelter in and around the incident area) and ensure the maintenance of those facilities. This unit's staff provide and maintain personnel support facilities, including areas for eating, sleeping, sanitation and showers, and staging.

Staff in this unit order additional support items such as portable toilets, shower facilities, and lighting units through the Supply Unit.

Facilities Unit

The Facilities Unit provides facilities that support incident personnel. Providing emergency shelter for survivors is a tactical activity for which the Operations Section, not the Logistics Section, is responsible.

Ground Support Unit

Ground Support Unit staff provide ground transportation in support of incident operations. They maintain and repair vehicles and mobile ground support equipment and perform pre- and post-use inspections on all ground equipment assigned to the incident. The staff supply fuel for incident mobile equipment, and develop and implement the incident Traffic Plan.

Additionally, during major incidents, Ground Support Unit staff maintain a transportation pool of vehicles (e.g., cars, buses, pickup trucks) suitable for transporting personnel, as opposed to tactical vehicles such as ambulances. Ground Support Unit staff also provide information to the Resources Unit on the location and status of vehicles assigned to the Ground Support Unit.

Communications Unit

Communications Unit staff install and test communications equipment, supervise and operate the incident communications center, distribute and recover communications equipment assigned to incident personnel, and maintain and repair communications equipment on site.

Most complex incidents have an incident Communications Plan. Staff in the Communications Unit produce this plan, as they are responsible for assigning radio frequencies; establishing voice and data networks for command, tactical, support, and air units; setting up on-scene telephone and public-address equipment; and providing any necessary off-incident communication links.

Food Unit

Food Unit staff determine the food and hydration needs of personnel assigned to the incident and plan menus, order food, provide cooking facilities, cook and serve food, maintain food service areas, and manage food security and safety.

Efficient food service is especially important for extended incidents. Food Unit staff anticipate incident needs, such as the number of people who will need to be fed and whether the incident's type, location, or complexity predicates special food needs. The unit staff supply food to meet the nutritional needs during the entire incident, including all remote locations (e.g., camps and

staging areas), and supply on-site food service to operations personnel who are unable to leave their assignments.

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

Food Unit

The Food Unit only provides food for incident workers. Feeding people affected by the incident (e.g., evacuees and persons at shelters) is a tactical activity for which the Operations Section, not the Logistics Section, is responsible.

Medical Unit

Medical Unit staff provide health and medical services for incident personnel. This includes providing pre-hospital and acute medical care, mental health care, occupational health support, and transportation of ill or injured incident personnel. The Medical Unit staff, in coordination with the Safety Officer, assist in controlling the transmission of disease among incident personnel.

The Medical Unit Leader develops a Medical Plan, which is part of the IAP. The Medical Plan provides specific information on medical assistance capabilities at incident locations, off-site medical assistance facilities, and procedures for handling medical emergencies involving incident personnel.

Medical Unit staff assist the Finance/Administration Section with the administrative needs related to injury compensation, including obtaining written authorizations, billing forms, witness statements, administrative medical documents, and reimbursement as needed.

Medical Unit

The Medical Unit provides medical services for incident personnel. Providing medical services for people affected by the incident (e.g., evacuees and persons at shelters) is a tactical activity for which the Operations Section, not the Logistics Section, is responsible.

ICS Tab 5—The Finance/Administration Section

The Incident Commander or Unified Command establishes a Finance/Administration Section when on-site financial and/or administrative services are needed to support incident management activities. Large or evolving scenarios generally involve significant funding from multiple sources. In addition to monitoring multiple sources of funds, the Finance/Administration Section Chief tracks and reports accrued costs to the Incident Commander or Unified Command as the incident progresses, allowing the Incident Commander or Unified Command to forecast the need for additional funds before operations are negatively affected. This is particularly important if significant operational resources are provided under contracts.

Figure A-10 illustrates the basic organizational structure for a Finance/Administration Section. When the Incident Commander or Unified Command establishes this section, the Finance/Administration Section Chief staffs these units as needed.

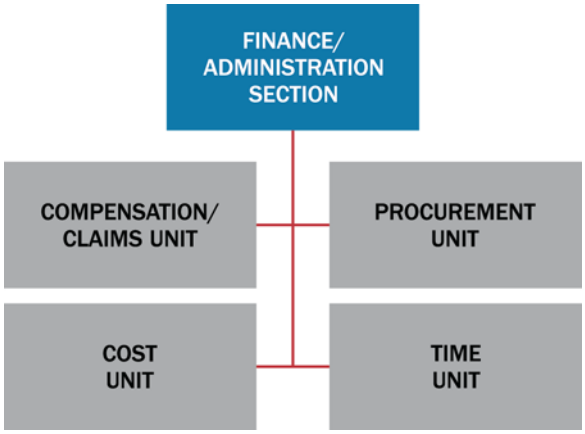


Figure A-10: Finance/Administration Section Organization

Finance/Administration Section Chief

The Finance/Administration Section Chief monitors expenditures to ensure compliance with applicable laws, policies, and procedures. Close coordination with the Planning and Logistics Sections is essential so that operational records can be reconciled with financial documents.

The Finance/Administration Section Chief determines—given current and anticipated future needs—the need for establishing specific subordinate units. Because of the specialized nature of finance functions, the Section Chief typically comes from the jurisdiction/organization that has the greatest need for this support. The Finance/Administration Section Chief may have one or more deputies or assistants.

Compensation and Claims Unit

Compensation and Claims Unit staff are responsible for financial concerns resulting from property damage, injuries, or fatalities at the incident. The specific activities vary depending on the incident. Staff handling injury compensation ensure that all forms needed by workers' compensation programs and local agencies are completed. These staff also typically maintain files on injuries and illnesses associated with the incident and obtain written witness statements. Since Medical Unit staff may also perform some of these tasks, the Medical and the

Compensation and Claims Units should coordinate closely. The Compensation and Claims Unit staff may assist with civil tort claims investigations involving incident property, and the staff maintain logs on the claims, obtain witness statements, and document investigations and agency follow-up activities.

Cost Unit

Cost Unit staff track costs, analyze cost data, make estimates, and recommend cost-saving measures. They ensure that equipment and personnel for which payment is expected are properly identified, obtain and record cost data, and analyze and prepare estimates of incident costs. Cost Unit staff provide cost estimates for resource use to Planning Section staff. The Cost Unit staff maintain information on the actual costs of all assigned resources.

Procurement Unit

The Procurement Unit staff administer all financial matters pertaining to leases and vendor contracts. Unit staff coordinate with local jurisdictions to identify sources for equipment, prepare and sign equipment rental agreements, and process documentation associated with equipment rental and supply contracts.

Time Unit

Time Unit staff ensure the daily recording of incident personnel and equipment time in accordance with the policies of the relevant agencies. The Time Unit Leader may need assistance from personnel familiar with the relevant policies of any affected agencies. Time Unit staff verify these records, check them for accuracy, and post them according to policies.

ICS Tab 6—The Intelligence/Investigations Function

The purpose of the intelligence/investigations function within ICS is to determine the source or cause of the incident (e.g., disease outbreak, fire, complex coordinated attack, or cyber incident) to control its impact and/or help prevent the occurrence of similar incidents. This involves collecting, analyzing, and sharing information and intelligence; informing incident operations to protect the lives and safety of response personnel as well as the public; and interfacing with counterparts outside the ICS organization to improve situational awareness.

These functions are typically performed by staff in the Operations and Planning Sections. However, for incidents that involve or may involve a significant level of intelligence/investigative work, the Incident Commander or Unified Command may choose to consolidate the intelligence/investigations function in the ICS organization in a number of ways. The intelligence/investigations function's location in the ICS structure depends on factors such as the nature of the incident, the level of intelligence/investigations activity involved or anticipated, and the relationship of the intelligence/investigations activities to the other incident activities. The intelligence/investigations function can be incorporated as an element of the Planning Section, in the Operations Section, within the Command Staff, as a separate General Staff section, or in some combination of these locations. Figure A-11 depicts the various locations where the Incident Commander or Unified Command might opt to locate intelligence/investigations function.

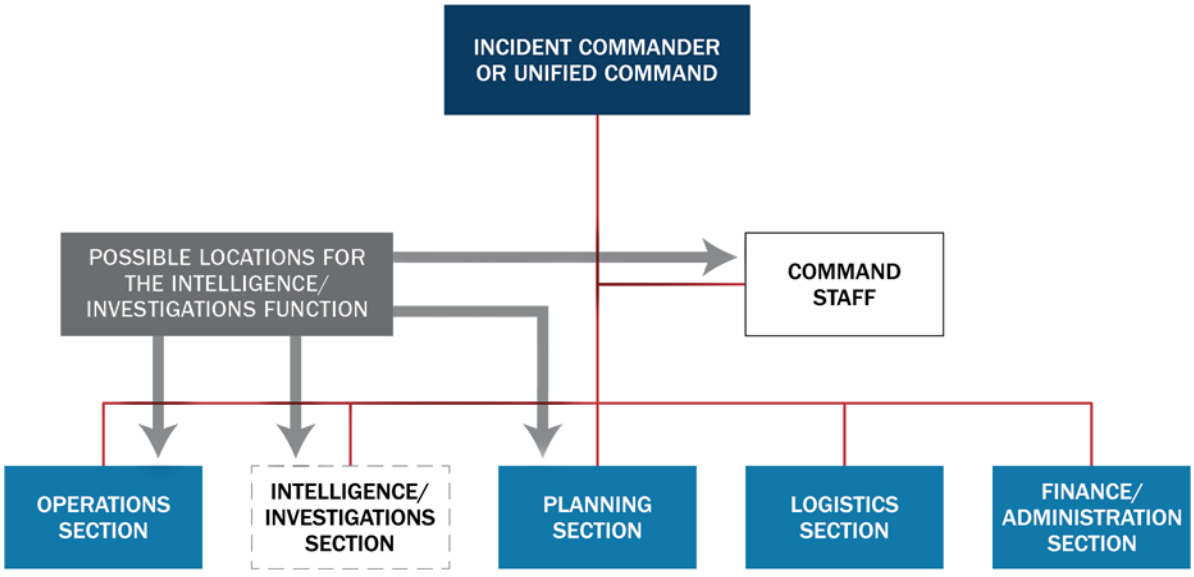


Figure A-11: Options for the Placement of the Intelligence/Investigations Function

Intelligence/Investigations Function in the Planning Section

Integrating the intelligence/investigations function in the Planning Section—either as part of the Situation Unit or as a separate Intelligence/Investigations Unit—enhances the section's normal information collection and analysis capabilities. It helps ensure that investigative information and intelligence is integrated into the context of the overall incident management mission. Intelligence/investigative staff benefit from access to Planning Section information management

resources and tools, and Planning Section staff benefit from streamlined information sharing and the analytic and subject matter expertise of the intelligence/investigations personnel.

Intelligence/Investigations Function in the Operations Section

The Operations Section typically integrates resources, capabilities, and activities from multiple organizations with multiple missions. Consolidating the intelligence/investigations activities in the Operations Section unifies all the incident operations (e.g., law enforcement, fire, EMS, hazardous materials response, public health, etc.) in one organization. This helps ensure that all incident activities are seamlessly integrated into the incident action planning process and conducted based on established incident objectives and priorities. This coordination enhances unity of effort, the effective use of all resources, and the safety and security of all incident personnel.

Within the Operations Section, the intelligence/investigations function may be configured as a new branch or group, integrated into an existing branch or group, or placed under the control of a new Deputy Operations Section Chief for Intelligence/Investigations.

As with all incidents, the leadership of the Operations Section should reflect the priority incident activities. During phases of incidents with extensive intelligence and investigative activities, such as a terrorist incident, intelligence/investigations personnel will dominate the Operations Section and should lead the section by filling the Operations Section Chief and other section leadership positions.

Intelligence/Investigations Function in the Command Staff

When the incident has an intelligence/investigations dimension but does not currently have active intelligence/investigations operations, the Incident Command or Unified Command may assign intelligence/investigations personnel to serve as command advisors. These technical specialists interface with their parent organizations and provide subject matter expertise to incident leaders. Integrating the intelligence/investigations function into the Command Staff helps ensure that the intelligence/investigations personnel have immediate and constant access to the Incident Commander, Unified Command, other members of the Command Staff such as legal advisors, the Safety Officer, and the PIO. This in turn helps ensure that incident leaders understand the implications and potential second-order effects of incident management decisions and activities from an intelligence/investigations standpoint.

Intelligence/Investigations Function as a Standalone General Staff Section

The Incident Commander or Unified Command may establish the intelligence/investigations function as a General Staff section when there is a need to manage the intelligence/investigations aspects of the incident separately from the other incident management operations and planning. This may occur when the incident involves an actual or potential criminal or terrorist act or when significant investigative resources are involved, such as for an epidemiological investigation.

The Intelligence/Investigations Section Chief leads the Intelligence/Investigations Section, which has groups for investigative operations, missing persons, intelligence, mass fatality management, forensics, and investigative support.[21]

Establishing the intelligence/investigations function as a General Staff section has the potential to create overlaps with the responsibilities of the Planning, Operations, and Logistics Sections. The Intelligence/Investigations Section Chief and other General Staff members should clarify expectations with the Incident Commander or Unified Command and coordinate closely to ensure that requirements are not lost or duplicated between sections.

[21] The National Incident Management System (NIMS) Intelligence and Investigations Function Guidance and Field Operations Guide describes the ICS intelligence/investigations function in more detail.

ICS Tab 7—Consolidating the Management of Multiple Incidents

Large disasters or multiple different disasters occurring quickly in the same area may result in the establishment of multiple incident command organizations operating more or less independently. ICS provides several options for consolidating the management of separate incidents. These options, which are described below, can enhance coordination and improve the efficient use of resources.

Incident Complex: Multiple Incidents Managed within a Single ICS Organization

An incident complex is an organizational structure that exists when two or more individual incidents located in the same general area are assigned to a single Incident Commander or Unified Command. When an incident complex is established over several individual incidents, the previously identified incidents become branches or divisions within the Operations Section of the incident complex. Each branch thus has the flexibility to establish divisions or groups. In addition, when divisions and groups have already been established at each of the incidents, the same basic structure can be propagated. If any of the incidents within an incident complex have the potential to become a large-scale incident, it is best to establish it as a separate incident with its own ICS organization.

The following are examples of when an incident complex may be appropriate:

- Disasters such as wildfires, earthquakes, tornadoes, floods, or other situations where many separate incidents occur in proximity;
- Several similar incidents occurring in proximity to one another; and
- One incident underway with an Incident Management Team (IMT) assigned, with other smaller incidents occurring in the same area.

The following are additional considerations for using an incident complex:

- A single Command and General Staff can adequately provide operations, planning, logistics, and finance/administration activities to the incidents that comprise the incident complex; and
- A combined management approach could achieve staff or logistical support economies.

Area Command

An Area Command is established to oversee the management and support of multiple incidents or to oversee the management of a large or evolving incident with multiple ICS organizations.

Area Command Responsibilities

An Area Command does not have operational responsibilities, but prioritizes the use of scarce resources among the incidents. Additionally, the Area Command:

- Develops broad objectives for the impacted area(s);
- Coordinates the development of individual incident objectives and strategies;
- Allocates resources as the priorities change;

- 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 EOCs and/or MAC Groups; and
- For incidents that have a recovery dimension, ensures that short-term recovery is coordinated to assist in the transition to full-recovery operations.

Area Command Organization

The Area Command organization operates under the same basic principles as ICS. Typically, an Area Command comprises the following key personnel:

- ***Area Commander (Unified Area Command)***: Responsible for the overall direction of assigned incidents. This responsibility includes ensuring that conflicts are resolved, incident objectives are established, and strategies are selected for the use of scarce resources. The Area Commander coordinates with local, state, tribal, territorial, and Federal departments and agencies, as well as NGOs and other private sector elements.
- ***Assistant Area Commander–Logistics***: Provides facilities, services, and materials at the Area Command level (by ordering resources needed to support the Area Command) and ensures the effective allocation of scarce resources and supplies among the incidents.
- ***Assistant Area Commander–Planning***: Collects information from various incidents to assess and evaluate potential conflicts in establishing incident objectives, strategies, and priorities for allocating scarce resources.
- ***Area Command Aviation Coordinator***: Assigned when aviation resources at multiple incidents compete for common airspace and scarce resources. This role works in coordination with incident aviation organizations to evaluate potential conflicts, develop common airspace management procedures, ensure aviation safety, and allocate scarce resources in accordance with Area Command priorities.
- Area Command Support Positions: Activated as necessary:
  - ***Resources Unit Leader***: Tracks and maintains the status and availability of scarce resources assigned to each incident under the Assistant Area Commander–Planning.
  - ***Situation Unit Leader***: Monitors the status of objectives for each incident assigned to the Area Command.
  - ***PIO***: Provides coordination between incident locations and serves as the point of contact for media requests to the Area Command.
  - ***Liaison Officer***: Helps maintain off-incident interagency contacts and coordination.

Area Command Location

The following are guidelines for locating an Area Command:

- Established as close to the incidents as needed to facilitate operations, to make it easier for the Area Commander and Incident Commanders or Unified Commands to meet and otherwise interact;
- Should not be co-located with any individual ICP, to avoid confusion with the ICP activities;
- Should allow for effective, efficient communications and coordination with subordinate incidents, as well as with EOCs and MAC Groups; and
- Housed in a facility large enough to accommodate a full Area Command staff. It should also be able to accommodate meetings among the Area Command staff, the Incident Commanders or Unified Commands, and agency administrators/executives as well as news media representatives.

Area Command Reporting Relationships

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

- The Incident Commanders for the incidents under the Area Command report to the Area Commander;
- The Area Commander is accountable to the agency or agencies or the jurisdictional executive(s) or administrator(s); and
- If one or more incidents within the Area Command are multijurisdictional, a Unified Area Command is established.

ICS Tab 8—Incident Action Planning

The incident action planning process and IAPs are central to managing incidents. The incident action planning process helps synchronize operations and ensure that they support incident objectives. Incident action planning is more than producing an IAP and completing forms—it provides a consistent rhythm and structure to incident management.

Personnel managing the incident develop an IAP for each operational period. A concise IAP template is essential to guide the initial incident management decision process and the continuing collective planning activities. The IAP is the vehicle by which leaders on an incident communicate their expectations and provide clear guidance to those managing the incident. The IAP:

- Informs incident personnel of the incident objectives for the operational period, the specific resources that will be applied, actions taken during the operational period to achieve the objectives, and other operational information (e.g., weather, constraints, limitations, etc.);
- Informs partners, EOC staff, and MAC Group members regarding the objectives and operational activities planned for the coming operational period;
- Identifies work assignments and provides a roadmap of operations during the operational period to help individuals understand how their efforts affect the success of the operation;
- Shows how specific supervisory personnel and various operational elements fit into the organization; and
- Often provides a schedule of the key meetings and briefings during the operational period.

The Incident Action Planning Process

The IAP provides clear direction and includes a comprehensive listing of the tactics, resources, and support needed to accomplish the objectives. The various steps in the process, executed in sequence, help ensure a comprehensive IAP. These steps support the accomplishment of objectives within a specified time.

The development of IAPs is a cyclical process, and personnel repeat the planning steps every operational period. Personnel develop the IAP using the best information available at the time of the Planning Meeting. Personnel should not delay planning meetings in anticipation of future information.

During the initial stage of incident management, the Incident Commander typically develops a simple plan and communicates the plan through concise oral briefings. In the beginning of an incident, the situation can be chaotic and situational awareness hard to obtain, so the Incident Commander often develops this initial plan very quickly and with incomplete situation information. As the incident management effort evolves, additional lead time, staff, information systems, and technologies enable more detailed planning and cataloging of events and lessons learned. The steps of the planning process are essentially the same for the first responders on scene determining initial tactics and for personnel developing formal written IAPs.

Planning "P"

Many incident management organizations use a formal planning cycle with established meetings and deliverables to mark their progress through the planning process and enable coordination of the entire team. The Planning P, illustrated in Figure A-12, is a graphical representation of the sequence and relationship of the meetings, work periods, and briefings that comprise the incident action planning cycle. Other versions of the Planning P may be used as training and operational aids.

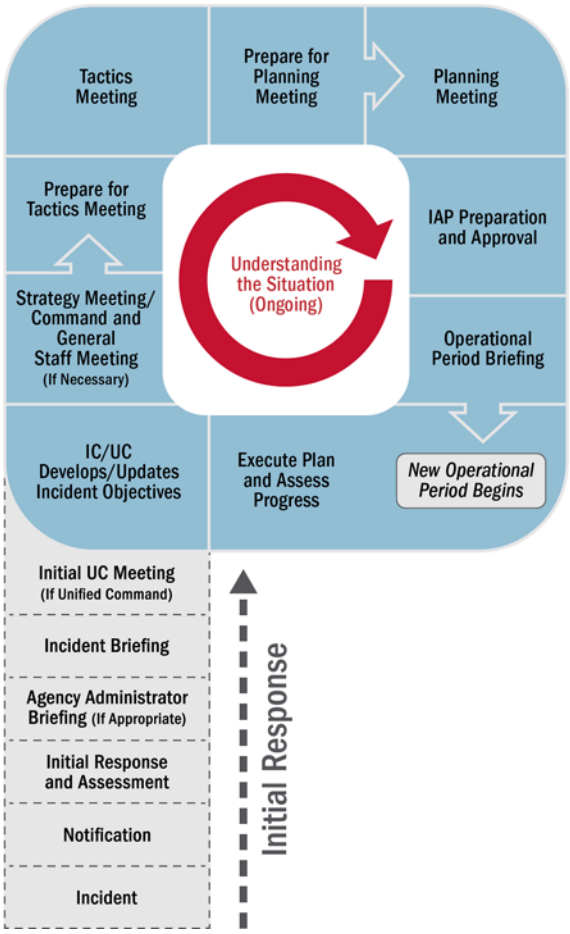


Figure A-12: Operational Period Planning Cycle

The leg of the "P" describes the initial stages of an incident, when personnel work to gain awareness of the situation and establish the organization for incident management. Incident personnel perform the steps in the leg of the "P" only one time. Once they are accomplished, incident management shifts into a cycle of planning and operations, informed by ongoing situational awareness and repeated each operational period.

Initial Response and Assessment

The responder(s) who is first to arrive at the incident scene conducts the initial assessment and takes whatever immediate response actions are appropriate and possible. The initial or rapid assessment is essential to gaining and maintaining situational awareness. It enables the Incident

Commander to request additional resources and/or support, develop, and implement initial tactics. Jurisdiction officials might decide to activate an EOC based on the initial assessment.

Agency Administrator Briefing

The Agency Administrator Briefing is a presentation to the personnel who will be managing or supporting the incident by the administrator or other senior official of the jurisdiction, agency, or organization affected by the incident. This briefing occurs when the Incident Commander or Unified Command are assuming duties outside their normal responsibilities or are from an entity or jurisdictional area that does not possess authority to the manage the incident they are being assigned. In such cases, the briefing provides supporting details to the delegation of authority or other document that the jurisdiction, agency, or organization typically provides to the Incident Commander or Unified Command.

During the briefing, the agency administrator or a designee provides information, guidance, and direction—including priorities and constraints—necessary for the successful management of the incident. The briefing is intended to ensure a common understanding between the jurisdiction, agency, or organization and the incident personnel regarding such things as the environmental, social, political, economic, and cultural issues relevant to the incident and its location.

Incident Briefing

The incident briefing marks the transition from reactive to proactive incident management. The initial responder(s) typically delivers the briefing to the incoming Incident Commander or Unified Command. This meeting enables the incoming Incident Commander or Unified Command to initiate planning for the next operational period.

Initial Unified Command Meeting

If a Unified Command is managing the incident, the Initial Unified Command Meeting allows members of the Unified Command to meet in private to discuss each jurisdiction or organization's priorities and objectives as well as any limitations, concerns, and restrictions. During the Initial Unified Command Meeting, members of the Unified Command generally accomplish the next step by developing the initial joint incident objectives.

Objectives Development/Update

The Incident Commander or Unified Command establishes the incident objectives for the initial operational period. After the initial operational period, the Incident Commander or Unified Command reviews the incident objectives and may validate them, modify them, or develop new objectives.

Incident objectives are based on incident priorities and other requirements. Clearly communicated priorities and objectives support unity of effort among incident personnel and enable the development of appropriate strategies and tactics. When the members of the team clearly understand the intent behind their instructions, they are better equipped to act decisively and make good decisions.

Strategy Meeting/Command and General Staff Meeting

After developing or revising the incident objectives, the Incident Commander or Unified Command typically meets with the Command and General Staff, and sometimes others, to

discuss the incident objectives and provide direction. This meeting may be called the Strategy Meeting or the Command and General Staff Meeting and is held as needed to determine how best to meet the incident objectives.

The initial Strategy Meeting, which is held the first time through the planning cycle, is particularly important, because it allows team members to share information and jointly determine the initial approach to response operations. The initial Strategy Meeting may include the initial Incident Commander and a representative from the Agency Administrator.

Preparing for the Tactics Meeting

Once the approach to achieving or working toward achieving the incident objectives is determined, the Operations Section Chief and staff prepare for the Tactics Meeting by developing tactics and determining the resources that will be applied during the operational period.

Tactics Meeting

The Tactics Meeting is a forum for key players to review the proposed tactics developed by the Operations Section staff and to conduct planning for resource assignments. The Operations Section Chief leads the Tactics Meeting, and key participants include the Logistics Section Chief, Safety Officer, a representative from the Planning Section—typically, the Resources Unit Leader—and other technical specialists or team members invited by the Operations Section Chief, Logistics Section Chief, or Safety Officer. The team uses ICS Forms 215 and 215A, the Operational Planning Worksheet and the Incident Action Plan Safety Analysis, to facilitate and document decisions they make during the meeting.

Preparing for the Planning Meeting

Following the Tactics Meeting, preparations begin for the Planning Meeting. Team members collaborate between the Tactics Meeting and the Planning Meeting to identify support needs and assign specific operational resources to accomplish the operational plan.

Planning Meeting

The Planning Meeting serves as a final review and approval of operational plans and resource assignments developed during and after the Tactics Meeting. Ideally, the Planning Meeting involves no surprises and simply serves as a review of a plan that the Command and General Staff have collaboratively developed and agreed upon. At the end of the Planning Meeting, Command and General Staff, and any agency officials involved, confirm that they can support the plan.

Table A-2 lists the elements responsible for completing each form for inclusion in the IAP.

Table A-2: The IAP and Typical Attachments

Component	Normally Prepared By ICS
Incident Objectives (ICS Form 202)	Incident Commander or Unified Command
Organization Assignment List or Chart (ICS Forms 203, 207)	Resources Unit
Assignment List (ICS Form 204)	Resources Unit
Incident Radio Communications Plan (ICS Form 205) Or Communications List (ICS Form 205A)	Communications Unit
Medical Plan (ICS Form 206)	Medical Unit
Incident Maps	Situation Unit
General Safety Message/Site Safety Plan (ICS Form 208)	Safety Officer
Other Potential Components	**(Incident Dependent)**
Air Operations Summary	Air Operations
Traffic Plan	Ground Support Unit
Decontamination Plan	Technical Specialist
Waste Management or Disposal Plan	Technical Specialist
Demobilization/Deactivation Plan	Demobilization Unit
Site Security Plan	Law Enforcement, Technical Specialist, or Security Manager
Investigative Plan	Intelligence/Investigations Function
Evacuation Plan	As needed
Meeting Schedule (ICS Form 230)	Situation Unit
Sheltering/Mass Care Plan	As needed
Other (as needed)	As needed

IAP Preparation and Approval

Based on concurrence from all elements at the end of the Planning Meeting, the Incident Commander or Unified Command approves the plan. After this final approval, the Planning Section staff assemble the plan and ensure that it is ready for use during the Operational Period Briefing.

A written IAP is composed of a series of standard forms and supporting documents that convey the intent of the Incident Commander or Unified Command, as well as the Operations Section

Chief for the operational period. The Incident Commander or Unified Command determines which ICS forms and attachments to include in the IAP; the Planning Section Chief ensures that staff in the appropriate sections, branches, or units prepare the forms and attachments. The Incident Commander or Unified Command gives final approval of the written IAP before Planning Section staff reproduce and disseminate it. IAPs may be distributed electronically, in hard copy, or both.

Operational Period Briefing

Each operational period starts with an Operational Period Briefing. Incident supervisory and tactical personnel receive the IAP during the briefing. During this briefing, various members of the Command and General Staff present the incident objectives, review the current situation, and share information related to communications or safety. Following the Operational Period Briefing, supervisors brief their assigned personnel on their respective assignments as documented in the IAP. During longer operational periods, shift change briefings may be conducted within an operational period.

ICS Tab 9—ICS Forms

This section describes common ICS forms. While the format and content are flexible, the form number and purpose (e.g., Assignment List, ICS Form 204, that defines the assignments for a division or group) should remain intact to maintain consistency, facilitate immediate identification and interoperability, and simplify their use.[22]

Not all ICS forms are included in the IAP; some support the planning process or incident operations in other ways. The IAP normally consists of the Incident Objectives (ICS Form 202), Organization Assignment List (ICS Form 203), an Assignment List (ICS Form 204) for each division/group on the incident, and a map of the incident area. Larger incidents necessitate additional supporting attachments, such as a separate Incident Radio Communications Plan (ICS Form 205), a Medical Plan (ICS Form 206), a Meeting Schedule (ICS Form 230), and possibly a Traffic Plan.

The following section provides brief descriptions of selected ICS forms. This list is not all-inclusive; other forms are available online, commercially, and in a variety of formats.

- ***ICS Form 201—Incident Briefing***: The initial Incident Commander typically uses this form to capture vital incident information before implementing the formal planning process. The use of this four-section document (often produced as four pages) allows a concise and complete transition-of-command briefing to an incoming new Incident Commander. In addition, this form may serve as the full extent of incident command and control documentation if the initial response resources and organization resolve the situation. This form simplifies and supports the transfer of situation information to the members of the Command and General Staffs as they arrive and begin work. It is not included as a part of a written IAP.
- ***ICS Form 202—Incident Objectives***: Serves as the opening section of a written IAP and includes incident information, a listing of the objectives for the operational period, pertinent weather information, a general safety message, and a table of contents for the plan. This form contains the signature block in which the Incident Commander or Unified Command approves the IAP.
- ***ICS Form 203—Organization Assignment List***: Is typically the second section of the IAP and provides a full accounting of incident management and supervisory staff for that operational period.
- ***ICS Form 204—Assignment List***: The incident IAP typically includes multiple ICS Form 204s, based on the organizational structure of the Operations Section for the operational period. Each division/group has its own page, listing the supervisor for the division/group (including the Branch Director if assigned) and the specific assigned resources with the leader's name and the number of personnel assigned to each resource. This document details the specific actions assigned to that division or group for the operational period, any special instructions, and pertinent elements of the Incident Radio Communications Plan (ICS Form 205).

[22] Template ICS forms can be found at https://www.fema.gov/incident-command-system-resources.

- ***ICS Form 205—Incident Radio Communications Plan***: Documents radio frequency assignments down to the division/group level.
- ***ICS Form 205A—Communications List***: Documents non-radio contact information for incident personnel.
- ***ICS Form 206—Medical Plan***: Presents the incident's plan to care for responder medical emergencies.
- ***ICS Form 207—Incident Organization Chart***: Depicts an organization chart of the major elements and key staff in the ICS organization.
- ***ICS Form 208—Safety Message/Plan***: Typically contains the safety message, expanded safety message, safety plan, and site safety plan.
- ***ICS Form 209—Incident Status Summary***: The primary form for reporting situation information to incident coordination and support organizations and agency administrators/executives.
- ***ICS Form 210—Resource Status Change***: Documents changes in the status of resources assigned to the incident; it can also be used as a worksheet to track resource arrival and departure.
- ***ICS Form 211—Incident Check-In List***: Documents resources that check in to the incident.
- ***ICS Form 213—General Message Form***: A general use form to communicate information among incident personnel or with other echelons of incident management.
- ***ICS Form 214—Activity Log***: Used to record notable activities or events.
- ***ICS Form 215—Operational Planning Worksheet***: Used to develop tactical assignments and identify resource needs for the coming operational period.
- ***ICS Form 215A—IAP Safety Analysis***: Communicates the safety and health issues identified by the Safety Officer; it also identifies mitigation measures to address safety issues.
- ***ICS Form 221—Demobilization Check-Out***: Documents details regarding the demobilization of incident resources.
- ***ICS Form 230—Meeting Schedule***: Records information regarding meetings and briefings scheduled for the operational period.

ICS Tab 10—Primary Functions of Incident Commander or Unified Command, Command Staff, and General Staff Positions

Table A-3 lists the primary functions of each major ICS position.

Table A-3: Summary Table of Major ICS Positions

Major ICS Position	Primary Functions
Incident Commander or Unified Command	• Have clear authority and know agency policy • Establish the ICS organization needed to manage the incident • Set incident objectives and determine incident priorities • Establish the ICP • Manage Command Staff and General Staff • Approve the IAP • Ensure incident safety • Approve resource requests and use of volunteers and auxiliary personnel • Authorize information release to the media • Order demobilization as needed • Ensure after-action reports are completed
Public Information Officer	• Develop accurate, accessible, and timely information for use in press/media briefings or dissemination via social media • Monitor information from traditional and social media that is useful for incident planning and forward it as appropriate • Understand any limits on information release • Obtain the Incident Commander's approval of news releases • Conduct media briefings • Arrange for tours and other interviews or briefings • Make information about the incident available to incident personnel • Participate in Planning Meetings • Identify and implement rumor control methods
Safety Officer	• Identify and mitigate hazardous situations • Stop and prevent unsafe acts • Create and maintain the incident Safety Plan • Prepare and communicate safety messages and briefings • Review the IAP for safety implications • Assign assistants qualified to evaluate special hazards • Initiate preliminary investigation of accidents within the incident area • Review and approve the Medical Plan • Participate in Planning Meetings to address anticipated hazards associated with future operations

Major ICS Position	Primary Functions
Liaison Officer	• Act as a point of contact for agency representatives • Monitor incident operations to identify current or potential inter-organizational issues • Maintain a list of assisting and cooperating agencies and agency representatives • Assist in setting up and coordinating interagency contacts • Participate in Planning Meetings and provide current resource status, including limitations and capabilities of agency resources • Provide agency-specific demobilization information and needs
Operations Section Chief	• Manage tactical operations • Determine strategies and tactics for incident operations • Ensure safety of tactical operations • Oversee the Operations Section's central role in the incident action planning process • Supervise execution of the Operations Section's assignments in the IAP • Request additional resources to support tactical operations • Approve release of resources from operational assignments • Make or approve expedient changes to the IAP • Maintain close contact with the Incident Commander, subordinate Operations personnel, and other agencies involved in the incident
Planning Section Chief	• Collect and manage incident-relevant operational data • Supervise/facilitate incident planning activities • Supervise preparation of the IAP • Provide resources input to the Incident Commander and Operations Section in preparing the IAP • Reassign out-of-service personnel within the ICS organization, as appropriate • Compile and display incident status information • Establish information needed and reporting schedules for units (e.g., Resources Unit, Situation Unit) • Determine need for specialized resources • Establish specialized data collection systems as necessary (e.g., weather) • Assemble information on alternative strategies • Provide periodic predictions on incident potential • Report significant changes in incident status • Oversee preparation of the Demobilization Plan
Logistics Section Chief	• Manage all incident logistics • Provide facilities, transportation, communications, supplies, equipment maintenance and fueling, food, and medical services for incident personnel and all off-incident resources • Identify known or anticipated incident service and support needs • Request additional resources as needed • Provide the Logistics Section's input to the IAP • Ensure and oversee development of Traffic, Medical, and Communications Plans as needed • Oversee demobilization of Logistics Section and associated resources

Major ICS Position	Primary Functions
Finance/ Administration Section Chief	• Manage financial aspects of an incident • Provide financial and cost analysis information as requested • Ensure compensation and claims functions are addressed relative to the incident • Develop an operational plan for the Finance/Administration Section and submit requests for the section's supply and support needs • Maintain daily contact with cooperating and assisting agencies on finance matters • Ensure that personnel time records are completed accurately and transmitted to the appropriate agency/organization • Ensure the accuracy of all obligation documents initiated at the incident • Brief agency administrative personnel on incident-related financial issues needing attention or follow-up • Provide input to the IAP

Appendix B. EOC Organizations

A. Purpose

This appendix provides additional explanation and examples of Emergency Operations Center (EOC) organizational structures commonly used in EOCs in the United States. They are not intended to be mandatory, definitive, or exclusive. Jurisdictions or organizations may choose to use one of these structures, a combination of elements from different structures, or an entirely different structure.

The description of each organization includes information on when and why a jurisdiction or organization might wish to use it and a description of the typical functions the various elements in the organization perform.

While it is not depicted on the various organizational graphics, EOCs are guided by policy groups that typically include elected and appointed senior officials such as governors, mayors, city managers, and tribal leaders.

B. Organization of This Appendix

This appendix contains the following tabs:

- Tab 1—Incident Command System (ICS) or ICS-like EOC Structure
- Tab 2—Incident Support Model (ISM) EOC Structure
- Tab 3—Departmental EOC Structure

EOC Tab 1—Incident Command System (ICS) or ICS-like EOC Structure

Many jurisdictions/organizations opt to use an ICS or ICS-like structure in their EOCs. This is typically because people are familiar with the structure, and it aligns with what is used in the field. Additionally, it is a useful functional breakdown, particularly for EOCs that might take on operational missions. ICS and EOC personnel may agree to adjust responsibilities among the organizations to meet incident needs and fulfill resource and information requests.

When using this type of EOC organization, field and EOC personnel performing the same function (e.g., Public Information Officer [PIO]) should agree on how to divide their responsibilities to avoid gaps and/or duplication of effort. Ideally, this coordination will occur before an incident, and the result will be documented in the jurisdiction/organization's emergency operations plan.

EOC leaders may opt for a standard ICS organization if:

- EOC staff are providing tactical direction to an incident;
- EOC management wishes to use ICS-trained personnel with no additional training requirements; or
- EOC managers want to mirror the organization of on-scene personnel.

Standard ICS Structure versus ICS-like Structure

If a jurisdiction/organization is using standard ICS, as practiced in the field, they will follow ICS procedures and processes as described in Appendix A. However, many EOC leaders find that modifying ICS slightly provides many of the benefits of the standard ICS structure while accommodating the differences between EOCs and Incident Command Posts (ICP).

An ICS-like EOC structure generally reflects the standard ICS organization but with varying nuances and possible title changes to emphasize the coordination and support mission of EOCs, as opposed to the tactical and logistics management role of on-scene responders. For example, EOC leaders often opt to adjust titles to differentiate between field and EOC functions/personnel by adding "Support" or "Coordination" to section titles (see Figure B-1). Additionally, some EOC leaders opt to modify certain ICS processes or functions to better reflect the activities and responsibilities of EOC personnel.

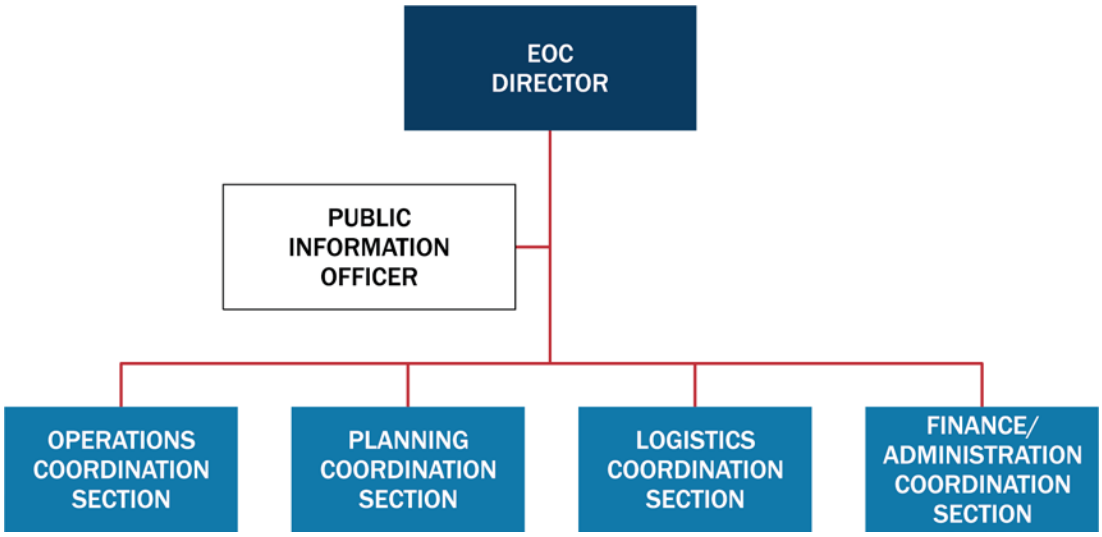


Figure B-1 : Example of an ICS-like EOC Organization Structure

EOC Command Staff

The EOC Command Staff (often called EOC Management Staff to clarify that they do not command on-scene operations) includes an EOC director who guides and oversees EOC staff and activities. The EOC Command Staff typically includes a PIO and may include others such as a Legal Advisor and a Safety Officer. The EOC director, possibly with the support of Command Staff, sets EOC objectives and tasks, integrates stakeholders, works with senior officials to facilitate the development of policy direction for incident support, and ensures the dissemination of timely, accurate, and accessible information to the public.

Operations Coordination Section

Operations Coordination Section staff help ensure that on-scene incident personnel have the resources and operational support necessary to achieve incident objectives and address leadership priorities. The staff in this section are often organized functionally—by Emergency Support Function (ESF) or Recovery Support Function (RSF), for example—and are the primary points of contact for on-scene response personnel within their respective functions. They coordinate closely with incident personnel to identify and address unmet resource needs. When necessary for geographically widespread or complex incidents or when establishing a local ICP is not possible, staff in the section can also support operational activity directly from the EOC.

Planning Coordination Section

The Planning Coordination Section has two primary functions: managing situational awareness efforts and developing activation-related plans. Staff in this section work closely with personnel in the ICS Planning Section to collect, analyze, and disseminate incident and incident-related information, including integrating geospatial and technical information and developing reports, briefings, and presentation products for a variety of stakeholders, including leadership, EOC personnel, and other internal and external stakeholders. Planning Coordination Section personnel also facilitate a standard planning process to achieve the EOC objectives and provide a range of current and future planning services to address current needs and anticipate and devise the means to deal with future needs.

Logistics Coordination Section

Logistics Coordination Section staff provide advanced resource support to the incident. They work closely with Operations Coordination Section staff to source and procure resources by implementing contracts or mutual aid agreements or by requesting other government assistance (e.g., local or tribal to state, state or tribal to Federal). Staff in this section also provide resources and services to support the EOC staff. This includes information technology (IT) support, resource tracking and acquisition, and arranging for food, lodging, and other support services as needed.

Resource Management in an ICS-like EOC

EOC leaders often adjust ICS resource management processes to fit an EOC environment better. The various departments and agencies represented in the Operations Coordination Section may have access to internal departmental resources that they can order without going through the Logistics Coordination Section. The Logistics Coordination Section may have expertise in advanced resource ordering, such as (1) through mutual aid, (2) by leasing or purchasing, or (3) through a request for assistance from a governmental organization (e.g., state or Federal support). The personnel in the Operations Coordination Section may be better positioned to track incident resources than personnel in the Planning Coordination Section. Staff in each EOC establish protocols on how to coordinate and track the resource ordering functions at the EOC and with field personnel.

Finance/Administration Coordination Section

Finance/Administration Coordination Section staff manage the activation's financial, administrative, and cost analysis aspects. Finance/Administration Coordination Section staff track all expenditures associated with the activation, including monitoring funds from multiple sources. Reporting on costs as they accrue enables EOC leadership to estimate needs accurately and request additional funds if needed. Finance/Administration Coordination Section staff may provide administrative support to other EOC sections. In some cases, the EOC Finance/Administration Coordination Section staff assume responsibilities of their ICS counterparts and perform functions on their behalf.

EOC Tab 2—Incident Support Model (ISM) EOC Structure

The ISM is a variation of the ICS structure that separates the information management/situational awareness function from the ICS Planning Section and combines the functions of the ICS Operations and Logistics Sections and comptroller/purchasing functions from the ICS Administration/Finance Section. EOC staff in jurisdictions or organizations that use an ISM structure typically focus exclusively on support functions rather than operations or managing actual response/recovery efforts.

As with the ICS/ICS-like model, the director of an ISM EOC is supported by personnel designated to key functions, subject matter experts, and technical specialists. Staff supporting the EOC director typically include a PIO and may include others such as a legal advisor. The General Staff sections consist of Situational Awareness, Planning Support, Resources Support, and Center Support. Figure B-2 shows a top-level management structure for an ISM EOC.

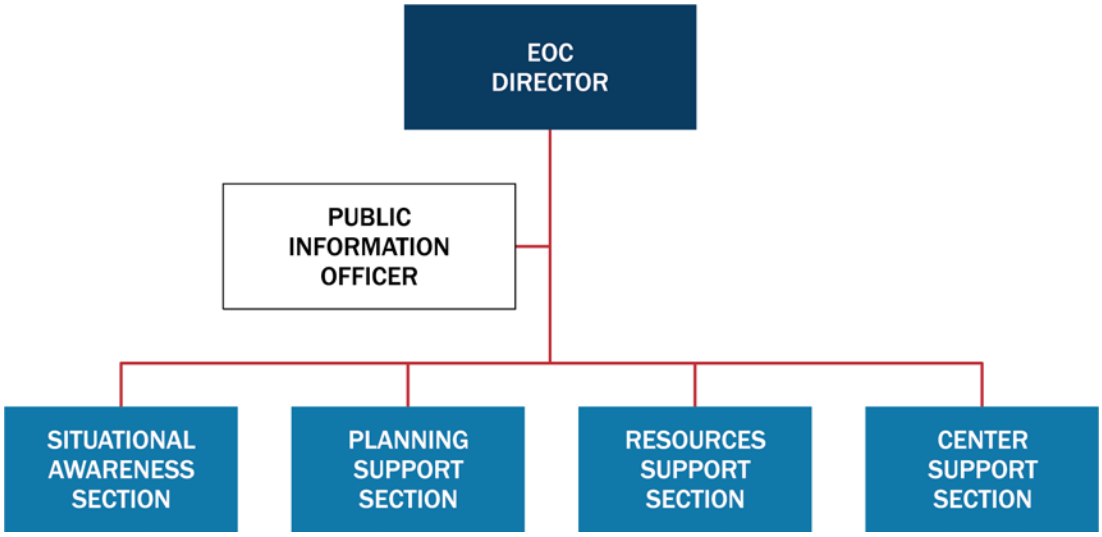


Figure B-2: Incident Support Model EOC Organization Structure

ISM EOC Director's Staff

As with the ICS/ICS-like EOC Command Staff, the ISM EOC director's staff typically includes a PIO and may include others such as a Legal Advisor and a Safety Officer. The EOC director and director's staff set EOC tasks, work with senior officials to facilitate the development of policy direction for incident support, and ensure the dissemination of timely, accurate, and accessible information to the public.

Situational Awareness Section

Situational Awareness staff collect, analyze, and disseminate incident information. This section's personnel typically create and provide a variety of products for EOC policy-level leadership, public affairs, and other internal and external stakeholders. The Situational Awareness Section essentially elevates the functions of the ICS Planning Section Situation Unit to a General Staff position in the EOC, reporting directly to the EOC director. The staff in this section also process requests for information; develop reports, briefings, and presentation products; integrate geospatial and technical information; and develop material to support public warning messages.

Staff in the Situational Awareness Section may include representatives or liaisons from ESF #15 – External Affairs.

Planning Support Section

The Planning Support Section staff provide a range of current and future planning services that may include developing contingency, deactivation, and recovery plans. Staff in the Planning Support Section assist in developing and executing the shared goals of multiple jurisdictions and organizations involved in managing the incident and coordinate a standard planning process to achieve the objectives of the EOC leadership and foster unity of effort among all organizations represented in the center. The Planning Support Section staff coordinate closely with the ICS Planning Section to ensure that both on-scene and EOC personnel have appropriate contingency plans in place.

Resources Support Section

Staff in the Resources Support Section work to ensure that on-scene incident management personnel have the resources and operational support they need. Resource Support Section staff source, request/order, and track all resources. This includes supplies, equipment, and personnel acquired from departments and agencies represented in the EOC, other community organizations, mutual aid/Emergency Management Assistance Compact (EMAC) sources, or nongovernmental partners, as well as items purchased or leased. Staff in the Resources Support Section may be organized by department/agency or by ESF/RSF.

Resource Management in an ISM EOC

The departments and agencies represented in an EOC generally have access to a variety of resources that are specific to the department or agency's responsibilities. A typical ICS Logistics Section has expertise in ordering resources through mutual aid, purchasing/contracting/leasing, or from external government organization via requests for assistance. Funding for purchases/contract/leases or reimbursement of expenses is usually handled in the ICS Administration/Finance Section. ISM EOCs combine all these functions in the Resources Support Section, which provides a one-stop shop for acquiring, deploying, and tracking resources and services.

Center Support Section

EOCs require a variety of communications, IT, administrative, and general services, as well as staff support, such as food, to function most effectively. Staff in the Center Support Section support the needs of the facility and staff in the EOC and any associated facilities such as a Joint Information Center (JIC). In this role, staff in the Center Support Section communicate and gather requirements for supplies, equipment, administrative processes, security, maintenance, and other logistics to ensure the EOC staff have the resources and capabilities required to perform their roles.

EOC Tab 3—Departmental EOC Structure

Jurisdictions or organizations may choose to retain the day-to-day relationships they have with the various departments and agencies that they also work with in responding to and recovering from incidents. These organizations or jurisdictions may configure the personnel who assemble in the EOC by the participants' departments, agencies, or organizations. Such departmentally structured EOCs typically require less training and emphasize coordination and equal footing for all departments and agencies. In this model, a single individual, either the jurisdiction or organization's emergency manager or another senior official, directly coordinates the jurisdiction's support agencies, nongovernmental organizations (NGO), and other partners. This model can also be organized using ESFs instead of departments. Figure B-3 presents an example of a Departmental EOC structure.

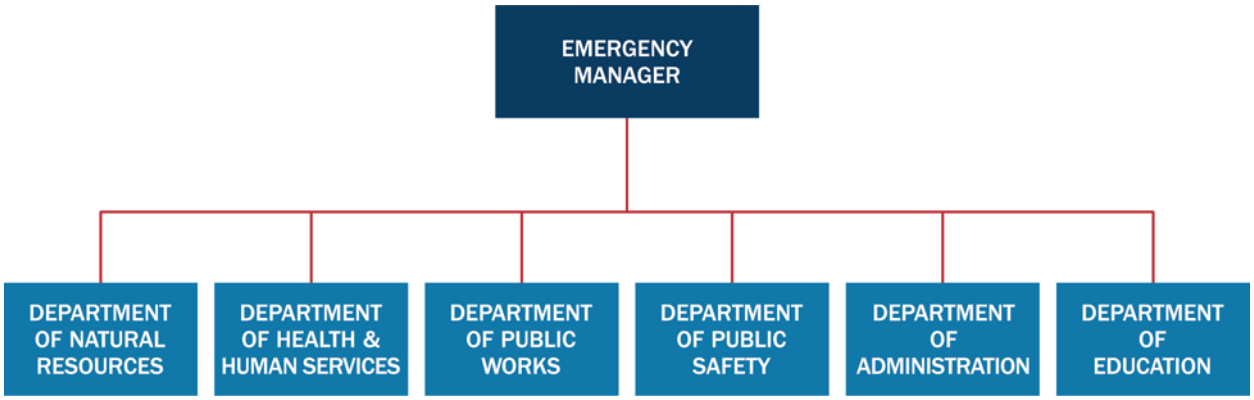


Figure B-3: Example of a Departmental EOC Organization Structure

In this example, the Emergency Manager, as EOC director, directly facilitates EOC planning and reporting. The EOC director may also be responsible for the office equipment, phones, radios, and/or computers in the EOC and ensuring food is available for the staff.

For the departments, representatives bring the various resources, expertise, and relationships that are associated with those organizations and functions. Decisions are made within the group to achieve mutually agreed-upon objectives, as in a Unified Command.

The roles and responsibilities of a departmental EOC reflect the day-to-day responsibilities of the represented departments and agencies. For example:

- EOC representatives from the department that deals with natural resources may be responsible, according to their normal authorities, for historic preservation, air and water quality, parks and recreation, game and wildlife, and wildfire suppression.
- Representatives in the EOC from the agencies that deal with public health, medical, and human services issues would be responsible for and provide resources associated with elder services; community hospitals, clinics, and medical services; sheltering and mass care; disease investigations; pharmacy services and mass dispensing sites; and liaison with humanitarian relief organizations.

- Representatives from public works are responsible for issues and resources in the EOC involving roads and grounds, sewers and sanitation, water purification, fuel, utilities, transportation, and solid waste.
- Police, sheriff, fire, and/or emergency medical services organizations all have representatives who coordinate their respective functions and resources in the EOC.
- EOC representatives from the jurisdiction or organization's administrative department or agency coordinate public information, finance, training, private sector and tribal liaison, and social/cultural centers.
- The public schools' officials assigned to the EOC are responsible for day care services, schools facilities (e.g., when used as emergency shelters), and school transportation.

These responsibilities would vary according to the jurisdiction's day-to-day departmental organization and responsibilities. This enables jurisdictions or organizations to address incidents effectively while maintaining their normal authorities, responsibilities, and relationships.