Incident Command System (ICS) Training Reference Guide

March 2023

FEMA

Preface

Incident Command System (ICS) Position Training courses teach individuals to perform key duties, responsibilities, and tasks as defined by the National Incident Management System (NIMS) and the National Qualification System (NQS) standard minimum position qualifications. These courses are intended for personnel who are regularly required to function under ICS, personnel who may be called upon to function in an ICS Command, Command and General Staff, Supervisor or Leadership position, or those persons who seek qualification in those positions. This includes, but is not limited to, individuals training to serve in rostered positions on a Type 3 Incident Management Team (IMT).

This *ICS Training Reference Guide* (Reference Guide) has been designed to serve as a companion document to the National Qualification System-based *Incident Command System Position Training Curriculum*. Students participating in the ICS Position Training will first use this Guide as a resource while attending the *IS-0995: ICS Position Training Foundations* course. This Guide serves as a companion textbook to the ICS Position Training courses. It also may be useful to those engaged in the qualification process for an ICS position to follow this training as a reference. The course will be designed in such a way that students will be able to use it to complete parts of the instruction, making the course an integrated learning experience. Throughout the course, students will be prompted to reference portions of this Reference Guide to support their completion of interactive activities in the course.

In addition to the *IS-0995: ICS Position Training Foundations* course, the Emergency Management Institute (EMI)'s *ICS Position* Training Curriculum currently consists of position-specific courses for key ICS supervisory positions. These courses provide local, tribal, territorial, state, and select Federal incident personnel with a robust understanding of the duties, responsibilities, and capabilities of ICS Command, Command and General Staff, Supervisor, or Leadership positions. Students will continue to use this Reference Guide during online and classroom sections of their position-specific training.

This Reference Guide will begin with a review of the National Incident Management System (NIMS) and the Incident Command System (ICS), as well as their characteristics, principles, and elements, to lay a foundation before delving into the details of the common duties and responsibilities for all ICS leadership positions. The remainder of this Reference Guide provides an in-depth look at ICS organizations and explores how ICS-based organizations fulfill their role in incident response and operational coordination.

Table of Contents

List of Figures

List of Tables

Chapter 1: Foundations

To understand the full extent of ICS organizations, it is important to understand how they fit into the bigger picture of the command and coordination of incident response. Knowing their place in the National Preparedness System and the National Response Framework will help set the foundational understanding of their purpose, functions, and importance. This chapter will set that foundation with a review of the National Incident Management System (NIMS) and the Incident Command System (ICS) as well as their guiding principles and structures.

Review of the National Incident Management System (NIMS)

Communities across the Nation experience a diverse set of threats, hazards, as well as events, and the size, frequency, complexity, and scope of these incidents vary, but they all involve a range of personnel and organizations to coordinate efforts to save lives, protect property and the environment, stabilize the incident, and meet basic human needs following an incident. 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. NIMS defines this comprehensive approach.

NIMS guides all levels of government, nongovernmental organizations (NGOs), 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 with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System. NIMS defines different operational systems, including the Incident Command System (ICS), Emergency Operations Center (EOC) structures, Multiagency Coordination Groups (MAC Groups), and the Joint Information System (JIS), and guides how personnel work together during incidents. NIMS is applicable to all incidents and events, from traffic accidents to major disasters and from a county fair to a National Special Security Event (NSSE). (NIMS, 2017)

The National Incident Management System (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, 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 an effort to make the ICS

guidance applicable to all types of incidents and all hazards. Under Homeland Security Presidential Directive (February 2003), the Federal government created the National Incident Management System (NIMS). This system directed the creation of a comprehensive, national approach to incident management. Recognizing the value of these systems, communities across the Nation have adopted NIMS. The most current revision of NIMS was released in October 2017. (ICS Review Document, 2018)

NIMS applies to all stakeholders with incident management and support responsibilities. The audience for NIMS includes emergency responders and other emergency management personnel, as well as non-governmental organizations (NGOs) (e.g., faith-based and community-based groups), the private sector, and the elected and appointed officials responsible for making decisions regarding incidents.

NIMS Guiding Principles

Incident management priorities include saving lives, protecting property and the environment, stabilizing the incident, and meeting basic human needs following an incident. To achieve these priorities, incident personnel apply and implement NIMS components in accordance with the NIMS Guiding Principles. These components include flexibility, standardization, and unity of effort.

Flexibility

NIMS components are *adaptable* to any situation, ranging from planned special events to routine local incidents to incidents involving interstate mutual aid or Federal assistance. Some incidents need multi-agency, multijurisdictional, and multidisciplinary coordination. Flexibility allows NIMS to be *scalable* and, therefore, applicable to 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 authority.

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
- Dispatch/Deployment
- Modular Organization
- Incident Action Planning
- Incident Facilities and Locations
- Integrated Communications
- Unified Command
- Accountability
- Information and Intelligence Management

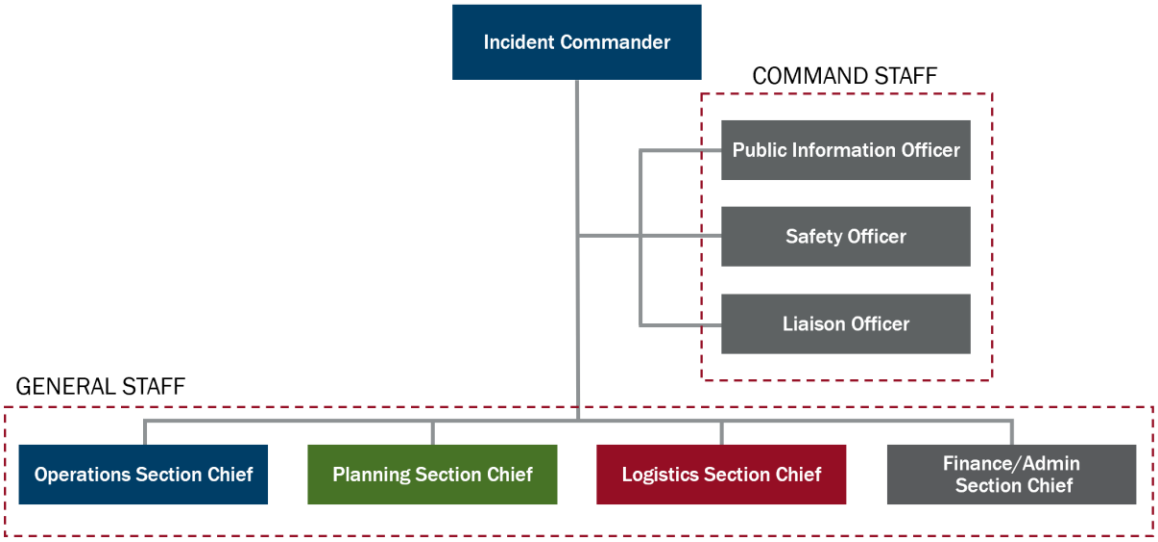
For access to the complete National Incident Management System (NIMS), visit: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf

Incident Command System (ICS)

ICS is a standardized approach to the command, control, and coordination of on-scene incident management. It provides a common hierarchy within which personnel from multiple organizations can be effective. ICS specifies an incident management organizational structure that integrates and coordinates a combination of procedures, personnel, equipment, facilities, and communications. (NIMS, 2017)

Using ICS for every incident helps hone and maintain the skills needed to coordinate efforts effectively. ICS is used by all levels of government, as well as many non-governmental organizations and private sector organizations. ICS can be applied across different disciplines and enables incident managers from different organizations to work together seamlessly. This system includes five major functional areas, staffed as needed, for a given incident. The functional areas are Command, Operations, Planning, Logistics, and Finance/Administration.

Figure 1: ICS Organization



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.

A sixth functional area, Intelligence/Investigations, is not present in all incidents. It is only used and staffed in incidents where it is required. It is placed within the ICS organization where it is best able to fulfill its specific function.

Overall ICS Organizational Functions

The Incident Command System (ICS) was designed by identifying the primary activities or functions necessary to effectively respond to incidents. Analyses of incident reports and reviews of military organizations were all used in ICS development.

As incidents become larger in scope, more complex, difficult, and expensive, the need for an organizational manager grows as well. Thus, in ICS, and especially in larger incidents, the Incident Commander manages the organization needed to respond and not the incident itself.

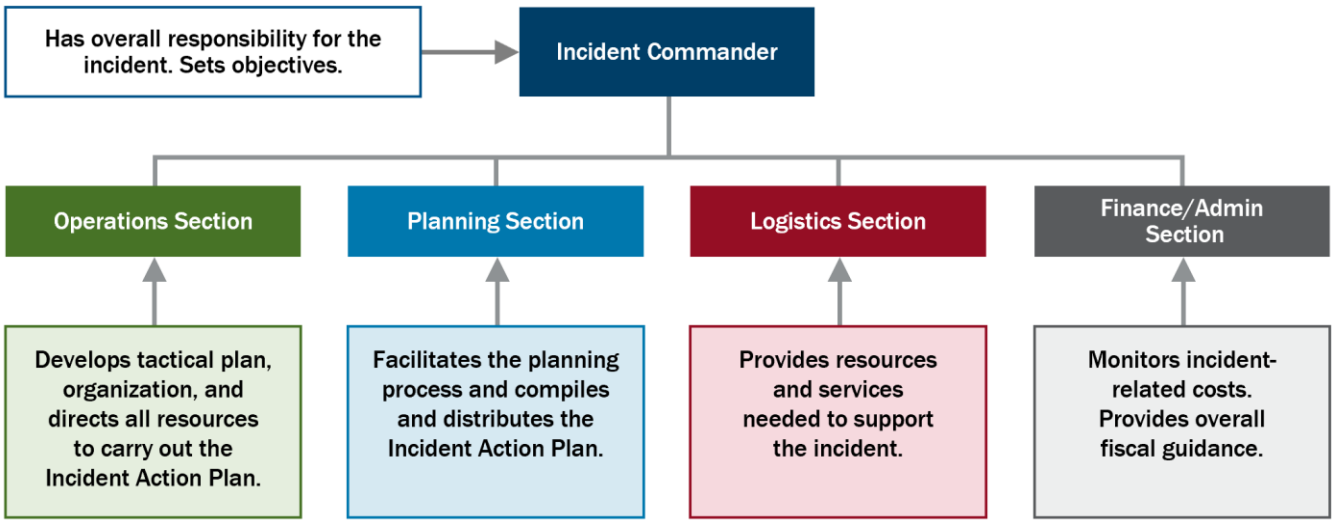
In addition to the Command function, other important functions and activities were identified, including:

- Delegating authority and establishing a separate organizational level that is solely responsible for the operational and tactical direction and control of resources within the ICS structure
- Providing planning services for both current and future activities
- Providing logistical support to the incident organization

- Providing planning services for both current and future activities
- Providing financial and administrative cost assessment, time recording, and procurement control necessary to support the incident and the managing of claims
- Promptly and effectively interacting with the media and providing information services for the incident, involved agencies, and the public
- Ensuring a safe operating environment within all parts of the incident organization
- Ensuring that assisting and cooperating agencies' needs are met and to see that they are used effectively
    - An assisting agency is an agency or organization providing personnel, services, or other resources to the agency with direct responsibility for incident management.
    - A cooperating agency is an agency supplying assistance other than direct operational or support functions or resources to the incident management effort.
- Managing intelligence or investigative functions when it is required in an incident

The structure of the major functional areas in an ICS organization is presented in Figure 2.

Figure 2: ICS Organizational Functions



Note: For more information on the placement of Intelligence/Investigations within the ICS structure, refer to the *Intelligence/Investigations Function* section of this guide.

ICS Functional Elements

Below are functional elements that will be referenced throughout this Reference Guide. It is important to understand that we are not yet discussing organizational structures such as

sections, branches, and units. We are instead discussing the functions that must be performed by the ICS organization.

The ICS functions must be managed regardless of whether a section, branch, or unit has been established. The ICS functions are staffed based on the nature and scope of the incident, the jurisdictions and organizations involved, and the incident's priorities, objectives, and strategies.

Responsibility for functions defaults to the next highest supervisory position until the supervisor delegates those responsibilities. If, for example, the Incident Commander does not delegate Planning responsibilities to someone else, then the Incident Commander must perform that function.

Incident Command

Incident Command is the organizational element within the ICS structure responsible for the overall management of the incident. It consists of the Incident Commander (or Unified Command structure). The Agency Administrator establishes the overall objectives through the leader's intent for the incident, and the Incident Commander or Unified Command develops detailed objectives and strategies to achieve the overall objectives. This typically focuses on saving lives, reducing the immediate hazard, protecting property and the environment, stabilizing the incident, and restoring normal operations.

Unified Command

Unified Command is a team effort, and this allows all agencies with legal, geographical, or functional responsibility to assign a representative for an incident to serve as a member of a Unified Command organization. The Unified Command establishes a common set of incident objectives based on the Agency Administrators' direction and objectives. This is accomplished without losing or giving up agency authority, responsibility, or accountability. Unified Command is a crucial element in increasing the effectiveness of multijurisdictional or multi-agency incident response. As incidents become more complex and involve more agencies, the importance of implementing a Unified Command is increased. Unified Command also assists in sharing the workload in extremely complex or evolving incidents which require a multitude of expertise and experience to manage.

Role of the Jurisdiction in Defining Incident Objectives

Normally, the Incident Commander/Unified Command does not develop incident objectives in a vacuum. Established jurisdictional policy or specific guidance from the Agency Administrator will establish an overall direction for managing the incident. These are often referred to as "Management Objectives." The Incident Commander or Unified Command then develops Operational objectives and strategies in accordance with this jurisdictional guidance or policy.

Operations Function

The Operations function focuses on the development and execution of tactics in support of the incident objectives set by the Incident Commander/Unified Command. Tactics describe how resources will be deployed and directed to accomplish the incident objectives. Personnel responsible for the Operations function direct all resources involved in carrying out the Incident Action Plan. This includes deciding how and where resources will be applied in the field to meet the incident objectives. The Operations function is usually managed by the Operations Section Chief; however, it may be directly led by the Incident Commander/Unified Command.

Key duties and responsibilities of the Operations function personnel include:

- Developing and implementing strategies and tactics to achieve the incident objectives
- Organizing the Operations function to best meet the incident's needs, maintain a manageable span of control, and optimize the use of resources
- Supporting Incident Action Plan (IAP) development for each operational period (an operational period is a time scheduled to execute a set of operational actions specified in the IAP)
- Directing the management of tactical activities on behalf of the Incident Commander or Unified Command

Incident operations can be organized and executed in many ways. When an Operations Section is established, the Operations Section Chief organizes and staffs the section based on the nature and scope of the incident, the jurisdictions and organizations involved, and the incident's priorities, objectives, and strategies.

The Operations function must be managed regardless of whether a section, branch, or unit has been established. Responsibility for functions that subordinates perform defaults to the next highest supervisory position until the supervisor delegates those responsibilities.

Planning Function

The Planning function collects, evaluates, and disseminates the incident situation information to the Incident Commander or Unified Command and other incident personnel. Planning staff prepares 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. The IAP is a vital document as it serves as an overall operational guide for both tactical and supporting elements of the organization.

Key duties and responsibilities of the Planning function personnel include:

- Facilitating the Incident Planning Process and its associated meetings and briefings
- Recording the status of resources and anticipated resource needs
- Collecting, compiling, displaying, and disseminating incident status information and analyzing the situation as it changes
- Planning for the orderly, safe, and efficient demobilization of incident resources.
- Collecting, recording, and safeguarding all incident documents

The Planning function must be managed regardless of whether a section or unit has been established. If the function has not been delegated, it remains the responsibility of the next highest supervisory position. If, for example, the Incident Commander does not delegate Planning responsibilities to someone else, then the Incident Commander must perform that function.

Logistics Function

The Logistics function provides services and support for effective and efficient incident management, including ordering resources and supporting resources. Planning staff provides 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.

Note: The Logistics function provides these services for incident personnel only. It does not provide these services for other non-incident personnel affected by the incident as those services fall to Operations.

The Logistics function staff's support to the ICS organization includes:

- Facilities
- Transportation
- Communications
- Supplies
- Equipment maintenance and fueling
- Food services (for responders)
- Medical services (for responders)
- All off-incident resources

Key duties and responsibilities of the Logistics function personnel include:

- Ordering, tracking, 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
- Providing medical services to incident personnel

The Logistics function must be managed regardless of whether a section or unit has been established. If the function has not been delegated, it remains the responsibility of the next highest supervisory position. If, for example, the Incident Commander does not delegate Logistics responsibilities to someone else, then the Incident Commander must perform that function.

Ordinarily, it is not an efficient use of the Incident Commander/Unified Command's time to review and approve all resource orders for routine supplies (e.g., food) on a major incident. The Incident Commander may delegate approval of certain orders while reviewing and approving any nonroutine requests, especially if they are expensive, require outside agency participation, or have potential political ramifications.

Finance/Administration Function

The Finance/Administration function provides 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. These actions must be closely coordinated with Planning and Logistics to align operational records with financial documentation.

The Finance/Administration function must be managed regardless of whether a section, branch, or unit has been established. If the Finance/Administration function has not been delegated, it remains the responsibility of the next highest supervisory position. If, for example, the Incident Commander does not delegate Finance/Administration responsibilities to someone else, then the Incident Commander must perform that function.

In large, complex incidents, Finance/Administration function staff must monitor and manage funding originating from multiple sources. The function's staff must also track and report the accrued costs of the entire incident response as it progresses. These actions allow the Incident Commander or Unified Command to forecast funding requirements and request additional funds as needed.

Key duties and responsibilities of the Finance/Administration function personnel include:

- Tracking costs, analyzing cost data, making estimates, and recommending cost-saving 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
- Recording time for incident personnel and leased equipment

Intelligence/Investigations Function

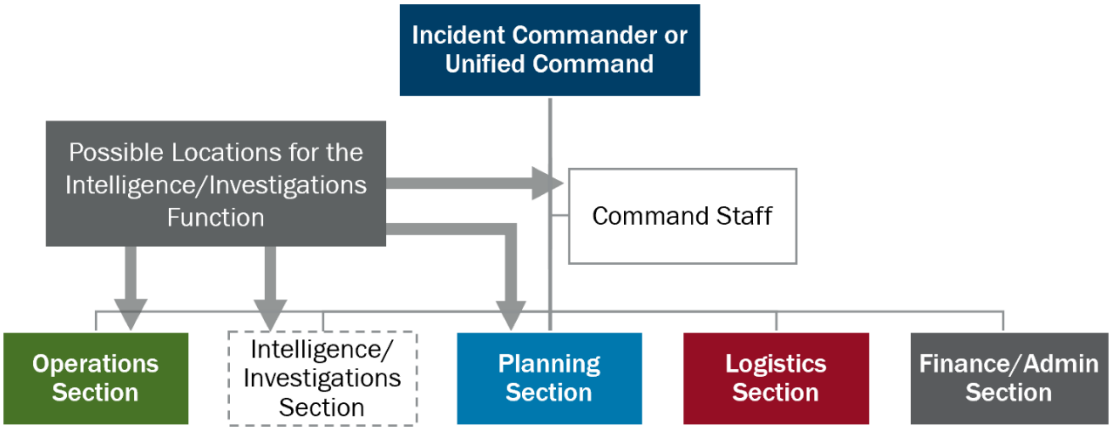
Intelligence/Investigations is a sixth ICS function. Unlike the five previous ICS functions, Intelligence/Investigations function is only utilized when required. To state this another way, an ICS organization will always perform the Incident Command, Operations, Planning, Logistics, and Finance/Administration functions, but it will only add the Intelligence/Investigations function when it is needed for the incident.

The collection, analysis, and sharing of incident-related information are important activities for all incidents. Typically, staff in the Planning function are responsible for gathering and analyzing operational information and sharing situational awareness, while staff in the Operations function are responsible for executing tactical activities.

However, some incidents involve intensive intelligence gathering (defined here as threat-related information developed by law enforcement, medical surveillance, and other investigative organizations) and investigative activity. For these incidents, the Incident Commander or Unified Command may opt to reconfigure intelligence and investigations responsibilities within the ICS structure to meet the needs of the incident. This may occur when the incident involves a criminal or terrorist act or other non-law-enforcement intelligence/investigations efforts such as epidemiological investigations.

The Incident Commander or Unified Command makes the final determination regarding the need for Intelligence/Investigations within an incident and, if needed, determines the scope and placement of the Intelligence/Investigations function within the ICS command structure. The Intelligence/Investigations function is a flexible concept in its application; when implemented, the Intelligence/Investigations function can be established as an element of the Planning function, in the Operations function, within the Command Staff, as a separate General Staff section, or in some combination of these locations. (NIMS, 2017)

Figure 3: Intelligence/Investigations Placement Options within the ICS Organization



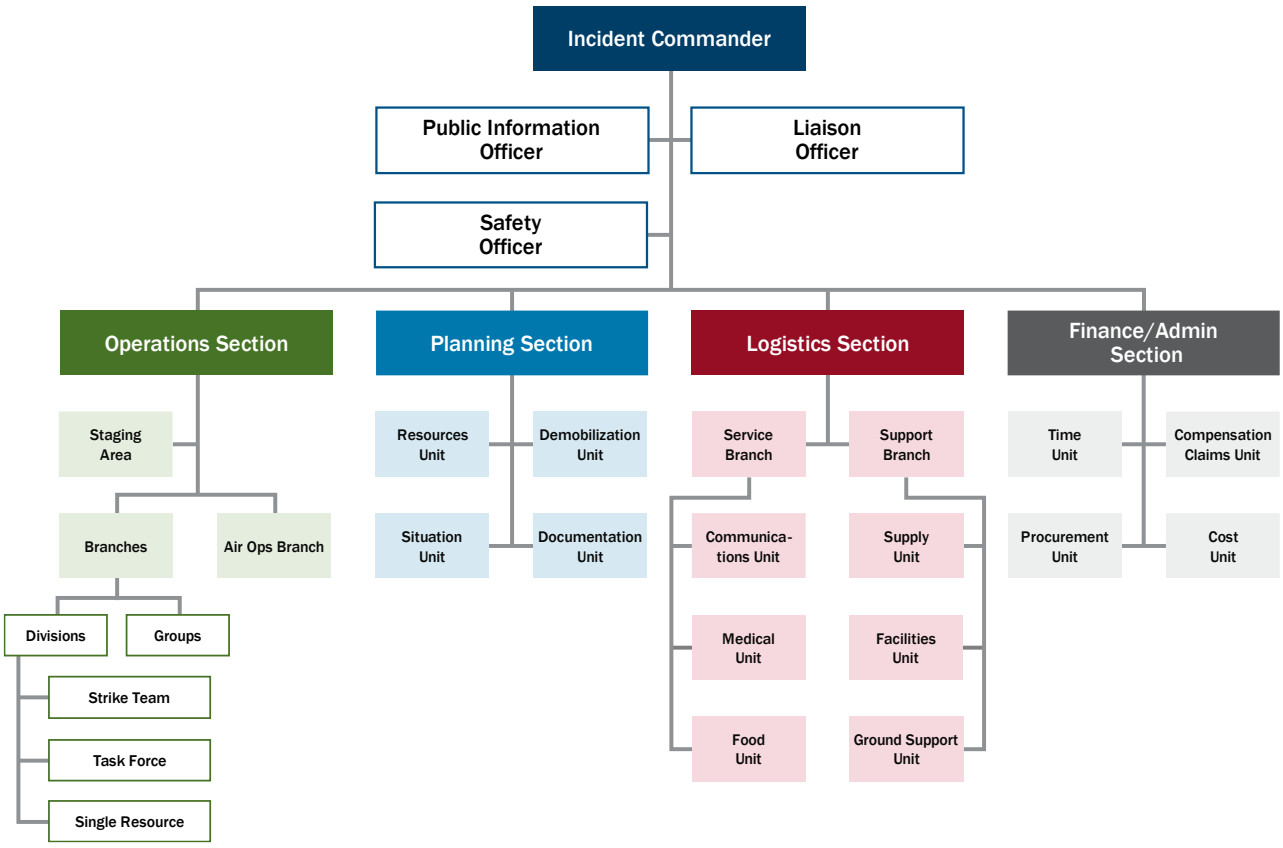
The purpose of the Intelligence/Investigations (I/I) function is to ensure that intelligence and investigative operations and activities are properly managed and coordinated to:

- 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, mass fatality, and 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 severity
- Determine the source or cause of an ongoing incident (e.g., disease outbreak, fire, complex coordinated attack, or cyber incident) to control its severity and/or help prevent the occurrence of similar incidents (NIMS, 2017)

Organizational Elements, Leadership Positions, and Support Positions

Below is an example of an organization chart with the major positions represented.

Figure 4: Expanded ICS Structure



At each level within the ICS organization, individuals with primary responsibility positions have distinct titles. Using specific ICS position titles serves these important purposes:

- Provides a common standard
- Ensures qualified individuals fill requested positions
- Standardizes communication
- Describes the responsibilities of the position

Table 1 explains the standardized NIMS position titles in the ICS structure.

Table 1: ICS Organization Position Titles

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

Key Parts of the Incident Command System

Incident Command/Unified Command: The organization responsible for the overall command and control/management of the incident (response and/or recovery, or event) within the mission, scope of work, and area of responsibility (AOR) to which the ICS organization is assigned.

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

Command Staff: The staff who report directly to the Incident Commander, including the Public Information Officer, Safety Officer, Liaison Officer, and other positions as required.

Section: The organizational level responsible for the major functional areas of incident management (e.g., Operations, Planning, Logistics, Finance/Administration, and Intelligence/Investigations, if established as a Section). Sections are organizationally situated between the Branch and the Incident Command levels.

Branch: The organizational level responsible for major aspects of incident operations on a functional and/or geographical level. A Branch is organizationally situated 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.

Division: The organizational level responsible for operations within a defined geographic area. For example, a Division could be established to manage tactical operations on the Southside of a river, and another Division established to manage operations on the Northside of that same river. The Division level is organizationally placed between the Strike Team and the Branch levels. Divisions are typically identified by letter (e.g., Div. A, Div. B).

Group: An organizational subdivision established to divide the incident management structure into functional areas of operation. For example, during an incident, fire suppression operations can be managed by one Group, while an arson investigation is managed by a separate Group. Groups are located between Branches (when activated) and resources (personnel, equipment, teams, supplies, and facilities) within the Operations Section. Groups are typically identified by their function (e.g., Traffic Control Group, Patient transportation Group).

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

Task Force: Any combination of resources of different kinds and/or types assembled to support a specific mission or operational need. A Task Force will contain *different kind*s and *type*s of resources (for example, fire engines and ambulances). All resource elements within a Task Force must have common communications and a designated leader.

Common examples would include an Arson Task Force comprised of fire, law enforcement, and other units from varying local, state, or national jurisdictions to investigate the cause of multiple large fires. Another common example would be a Debris Management Task Force comprised of public works, law enforcement, private contractors, and fire support to manage removing debris that is blocking vital public safety routes or access to hydrants or other utilities.

Strike Team/Resource Team: A Strike Team consists of a certain amount of resources of the *same kind* and *type* (for example, all the same kind and type of ambulance) that have an established minimum number of personnel, common communications, and a designated leader (i.e., 5 Type-1 Engines with 20-personnel, 5 ALS ambulances with 10-personnel). It is used for rapid response and is established to meet particular tactical needs.

In some organizations, such as the law enforcement community, Strike Teams are sometimes referred to as Resource Teams. A Resource Team consists of a certain number of law enforcement resources of the *same kind* and *type,* with an established minimum number of personnel (i.e., five patrol cars with two officers each – 10 personnel).

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

Staging Area(s): A temporary location managed by the Operations Section. A staging area can be any location in which personnel, supplies, and equipment await assignment. The Operations Section Chief assigns a manager for each staging area who logs in all incoming resources, dispatches resources at the section chief's request, and requests Logistics Section support, as necessary, for resources at the staging area. The position in charge of the staging area is the Staging Area Manager.

Incident Life Cycle Phases

Phase 1 – Pre-Incident Actions that Shape Operations

Individuals qualified for ICS positions must be prepared to deploy to any type of incident at any time. Planning is a crucial step in ensuring a successful incident response. The National Fire Protection Association has developed a Standard for Pre-Incident Planning (NFPA 1620) to assist responders with pre-incident planning for fire disasters. This may be useful for pre-incident planning for other types of incidents as well. However, some agencies and organizations may have their own policies and procedures that need to be followed. Many communities have established Incident Management Teams to assist with local events or critical incidents. There are many advantages to having pre-established teams with policies and procedures who routinely meet and train together. This pre-incident planning establishes a ready-to-go cohesive group of multi-jurisdictional responders who can assist in response and recovery operations. Jurisdictions should have existing emergency plans that identify how the jurisdiction will respond to incidents. These plans may have functional or hazard-specific annexes that address specific hazards or types of disasters. Command and General Staff especially should be familiar with these plans for the jurisdiction(s) in which they are operating. This is particularly relevant to incident management personnel (rostered or otherwise) associated with the jurisdiction.

Phase 2 – Activation, Deployment, and Sustained Response Operations

The requesting agency/jurisdiction will establish an ICS organization that is sufficient to manage the incident. ICS organizations "Typed" are usually aligned with the event based on the incident's complexity (i.e., Type 3 IMT for Type 3 incident complexity). Specifics of the request for the ICS organization may include the desired type and staffing, location, type of incident, mission, and requested arrival.

Note: Many ICS organizations are not standing teams or standing duty/on-call rotations. As such, each jurisdiction must develop policies and procedures that allow the efficient activation and deployment of an ICS organization. The ICS organization should utilize a standardized methodology during activation and mobilization for deployments. Each team member has common responsibilities that they carry out during the incident. In addition,

specific section chiefs, unit leaders, or designees have additional responsibilities, and these are outlined in Position Task Books, as well as position-specific training. This will include Emergency Operations Plans (EOPs), which should contain procedures for the activation and notification of essential incident personnel.

Phase 3 – Long-Term Sustained Operations

The initial operational periods may be challenging for the ICS organization as incidents and transitions are dynamic. However, the ICS organization will continue to use strong management and a deliberative planning process to be more proactive and prepared. In addition to updated strategies and tactics for each operational period, the ICS organization will also work towards enhancing situational awareness, common operating picture, and communications, both internal as well as external, while taking into consideration resource management and contingency plans.

Incident Complexity

Incident Complexity is the combination of involved factors that affect the probability of control of an incident (NIMS, 2021). Many factors determine the complexity of an incident, including, but not limited to:

- Area involved
- Threat to life and property
- Political sensitivity
- Organizational complexity
- Jurisdictional boundaries
- Values at risk
- Weather
- Strategy and tactics
- Agency policy

Incident complexity is part of the incident assessment and is a factor that is considered when the Incident Commander or Unified Command makes staffing and safety decisions.

Incident Typing

"Typing" an incident is not a mathematical equation. Typing an incident is both an objective and subjective assessment made by the Agency Administrator, Incident Commander, or Unified Command based on their analysis of the incident. Assigning a "Type" number to an incident can help communicate the incident's complexity using a common language. Even more important than determining the incident complexity type (assigning a type number) is the analysis of the factors that led to the complexity typing. The identification and analysis of the factors contributing to the incident's complexity will help the Incident Commander or

Unified Command determine the necessary objectives, strategies, tactics, resources, and ICS organization needed to resolve the incident.

Complex Incidents are larger incidents with higher incident complexity (normally Type 1 or Type 2 incidents) that extend into multiple operational periods and rapidly expand; they commonly require multijurisdictional and/or multidisciplinary efforts and require outside coordination, support, and resources.

Several tools have been developed to assist in examining the factors to consider when determining incident complexity, including:

Incident Complexity Analysis (USCG ICS 239 Form 239) - https://homeport.uscg.mil/Lists/Content/Attachments/2914/ICS239-CG%20DRAFT%20Incident%20Complexity%20Analysis.pdf

National Geographic Area Coordination Center - https://gacc.nifc.gov/rmcc/administrative/mob_guide/forms/Incident_Complexity_Analysis.doc

Table 2 Incident Complexity Level: Incident Effect Indicators Summary

Type	Resistance to stabilization or mitigation	How long does it take for resources to meet incident objectives?	Effects on population immediately surrounding the incident	Length of incident effects	Evacuations necessary during mitigation	Adverse impact on CIKR	CIKR impact/mitigation measures	Coordination required with elected/ governing officials and stakeholder groups	Do conditions or actions that caused original incident persist?	Probability of cascading event or exacerbation of current incident
5	None	1-2 hours	Minimal	Minimal	Few or none	None	None	Minimal or none	No	None
4	Low	Several to 24 hours	Limited	Up to 24 hours	Few or none	Minimal	Uncomplicated within one operational period	Minimal or none	No	Low to none
3	Moderate	At least 24 hours	Moderate	Several days to over one week	Possible; may require shelter	Threatens, damages, or destroys property	Adverse; multiple operational periods	Some	Possibly	Medium
2	High	Several days	Significant	Several days to two weeks	Possible; may require shelter/ housing for several days to months	Threatens, damages, or destroys property	Destructive; requires coordination over multiple operational periods	Moderate, including political organizations	Possibly	High
1	High	Numerous operational periods	Significant	Two weeks to over a month	May require shelter/ housing for several days to months	Significantly threatens, damages, or destroys property	Highly destructive; requires long-term planning and extensive coordination over multiple operational periods	High, including political organizations	Yes	High

Incident Complexity and Levels

Incident Complexity

Incident complexity is the combination of involved factors that affect the probability of control of an incident. Many times, we refer to this as "How big is big and how bad is bad." Incident complexity is considered when making incident management level, staffing, and safety decisions.

Several analytic tools have been developed to assist in the examination of important factors involved in incident complexity. Incident Complexity Analysis is covered in greater detail in Chapter 5 *Initial Response*.

Incident Typing Levels

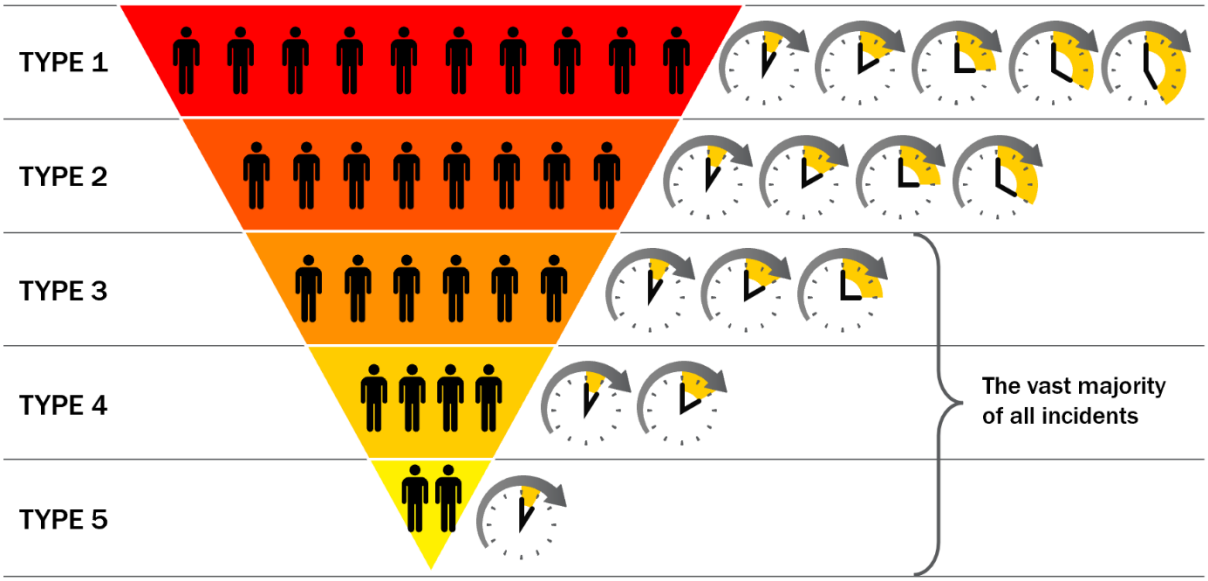
Incidents are categorized into five "types" based on their complexity. Type 5 incidents are the least complex, and Type 1 incidents are the most complex.

Incident typing may be used to:

- Communicate the complexity of an incident in a common language.
- Identify the factors contributing to incident complexity; this must be addressed in the incident objective, strategies, and tactics.
- Assess the organizational structure and staffing required to manage the incident.
- Prioritize incidents and resource allocation.
- Make decisions about resource requirements.
- Order Incident Management Teams (IMTs).

Figure 5 depicts the relationship between time, resources, and incident type. More complex incidents take longer to resolve, require more resources, and use a larger ICS staff to manage. The vast majority of incidents are relatively small.

Figure 5: Time and Resource Requirements Based on Incident Type



Resource Typing

Resources can also be typed to reduce confusion in resource requests. Resource typing is the categorization and description of resources that are commonly exchanged in disasters via mutual aid. Typing is done to ensure that responders get the right personnel and equipment. Resources are categorized by capability, category, kind, and type.

- Capability. The core capability for which a resource is most useful.
- Category. The function for which the resource is most useful.
- Kind. A description of what the resource is (personnel, teams, facilities, equipment, or supplies).
- Type. The minimum capability of a resource to perform its function is based on size, power, and capacity (for equipment) or experience and qualifications (for personnel or teams).

Resource typing definitions establish a common language and define the minimum capabilities for each resource (equipment, teams, or units).

For up-to-date information on NIMS Components – Guidance and Tools, go to: https://www.fema.gov/emergency-managers/nims/components.

Importance

Resource typing definitions help define resource capabilities for ease of ordering and mobilization during an incident. During a disaster, an emergency manager knows what

capability a resource needs to have to respond efficiently and effectively. As a result of the resource typing process, a resource's capability is readily defined, and an emergency manager can effectively and efficiently request and receive resources through mutual aid during times of disaster.

Resource Typing Tools

Resource Typing Definitions are provided for equipment, teams, and units. They are used to categorize, by capability, the resources requested, deployed, and used in incidents. This categorization is based on measurable standards that identify resource capabilities and performance levels. Job Titles/Position Qualifications (FEMA 509s) are used in the inventorying, credentialing, and qualifying of personnel. Credentialing is essential in validating the identity and attributes (e.g., affiliations, skills, or privileges) of emergency personnel. Position Task Books document the successful completion of tasks specific to a NIMS Incident Command System (ICS) position. The performance criteria for each position are associated with core ICS competencies, behaviors, and tasks.

For access to FEMA's online Resource Typing Library Tool, go to: https://rtlt.preptoolkit.fema.gov/public. Also, refer to National Resource Hub at https://preptoolkit.fema.gov/web/national-resource-hub for a suite of web-based tools that support a consistent approach to the resource management preparedness process.

Command, Coordination, and Oversight

Command

NIMS defines Command as the act of directing, ordering, or controlling by explicit statutory, regulatory, or delegated authority. Under NIMS/ICS, the Incident Commander or Unified Commanders have command authority over the incident. This authority is given to the Incident Commander or Unified Command by the Agency Administrator with authority over the jurisdiction. Incident Commanders, Unified Commands, and Area Commands are all entities that have command authority. NIMS points out that in some incidents, an EOC may manage certain operations, such as shelters or points of distribution, to allow the Incident Command to focus on the incident. There can also be incidents, such as a snow emergency, in which an Incident Command is not established; in these situations, the EOC may direct tactical operations. Coordination entities such as Emergency Operations Centers (EOC) and Departmental Operations Centers (DOC) are not normally given command authority.

Coordination/Support

Coordination is defined as "the organization of the different elements of a complex activity to enable them to work effectively." (Oxford Learner's Dictionary, 2021) This collaboration and

support for the incident provide a "unity of effort" between the Incident or Area Command, the EOC, the MAC Group/Policy Group, the JIC, and various levels of government (e.g., local, state, Federal).

Oversight

It is provided by the Agency Administrator/Agency Executive (or designee) to ensure the Incident Command is safely, effectively, and efficiently managing the incident and meeting the priorities, expectations, constraints, and other considerations or guidelines that were defined in the Delegation of Authority. Remember that the incident command authority is given to the Incident Commander or Unified Command, and if implemented, the area command by the senior elected or appointed official has jurisdictional authority. This effort starts with either a standing, pre-existing delegation of authority or a delegation of authority given in the Agency Administrator briefing during the initial response. The Agency Administrator provides policy guidance and resource prioritization and allocation until the closeout of the incident, regardless of the number and type of command structures used during the incident.

Unified Command

Unified Command (UC) is an ICS application frequently used when more than one jurisdiction, agency, or organization has primary authority. Private sector companies may also be part of Unified Command if they are deemed the "responsible party" and are participating in the response. Unified Command brings together the designated representatives of major organizations with either geographical or functional responsibility for the incident to manage an effective response while retaining their normal authority. Not every agency with resources involved in an incident would be a member of a Unified Command; this organizational structure may be more effective if there are a limited number of jurisdictions, agencies, or organizations participating as members of the Unified Command.

While the members of the Unified Command may designate an individual to speak for the Unified Command in meetings and briefings, none of the members of the Unified Command are the Incident Commander. Instead, the members of the Unified Command, working as a team, perform the Incident Command function together.

Members of the Unified Command work together to develop a common set of incident objectives, share information, maximize the use of available resources, and enhance the efficiency of the individual response organizations. This is accomplished without losing or abdicating jurisdictional, agency or organizational authority, responsibility, or accountability.

Note that while the Unified Command is a team that performs the Incident Command function, together, they direct a single Command and General Staff to carry out the other incident management functions.

The following criteria should be met for inclusion as a member of the Unified Command:

- The jurisdiction/agency/organization has the statutory or jurisdictional authority or functional responsibility under law or ordinance. This can include a Private Sector company that is identified as the Responsible Party in an incident.
- The jurisdiction/agency/organization is specifically charged with commanding or managing a major aspect of the response.
- The incident has a significant impact on the jurisdiction's/agency's/organization's area of responsibility.

Purpose of Unified Command

Unified Command is designed to bring all major jurisdictions/agencies/organizations that have authority/responsibility for the incident together to manage the incident collaboratively and cohesively. This prevents jurisdictions/agencies/organizations from responding in a unilateral, uncoordinated, and possibly ineffective manner.

Examples of Unified Command

- An oil tanker vessel attempting to moor has collided with the pier and sustained significant damage. A considerable amount of crude oil has leaked and continues to discharge from the vessel. Local Fire and Hazmat units have responded to mitigate the incident. Law enforcement has evacuated the workers from the area and secured the perimeter. The shipping company and Port Authority have activated their environmental clean-up contractors. The U.S. Coast Guard (USCG) has restricted access to the port and established a security zone on the water. The USCG Captain of the Port is responding to the scene. The state Department of Environmental Quality is en route as well. The Unified Command members could include:
    - United States Coast Guard (Federal Coordinating Officer)
    - State Department of Environmental Quality (State Coordinating Officer)
    - City representative responsible for fire, Hazmat, law enforcement, and port authority
    - Ship's owner as the responsible party
- An active shooter incident occurred in a local high school. There were approximately 1,000 students plus teachers and staff in the school at the time of the incident. Local law enforcement responds to the active shooter incident, and SWAT is en route. State troopers are securing the outer perimeter. EMS and fire units are treating patients

that have exited the school and are standing by to treat others in the school. Several FBI special agents are en route. Students that were able to evacuate the school are being secured in an adjacent middle school that is locked down. The Unified Command members could include:

- Law Enforcement
- EMS/Fire
- School Principal or District (Responsible for all students and reunification with parents)
- FBI representative if the incident is determined to be a terrorist incident

Coordination Entities

Emergency Operations Center

Emergency Operations Centers (EOC) are offsite locations (away from the incident or event scene) where staff from multiple agencies and/or disciplines assemble to provide coordinated support for on-scene ICS operations during a significant incident or event. EOCs also help to ensure the continuity of services and governance of the impacted community. EOCs are multi-agency, multi-discipline coordination entities. The purpose, authorities, and composition of EOCs vary widely. However, in most jurisdictions, they do not routinely have command authority.

EOC facilities can be fixed, temporary, or virtual. They consolidate and exchange information, support decision-making, coordinate resources, and communicate with personnel on-scene (Incident Command/Unified Command), Area Commands, and other Coordination Centers (such as Departmental Operations Centers or Business Operations Centers). The EOC also supports the information, decision support, and policymaking activities of the Multi-Agency Coordination Group (MAC Group) and normally is an intermediary for situational awareness and policy communication between the Incident Command/Unified Command and the MAC Group. Departmental Operations Centers tend to focus solely on operations involving that one governmental entity, while Business Operations Centers perform a similar function for industry, where the need for internal collaboration is required to address a specific issue or impact. ICS-trained personnel can fill positions in the EOC and support response and recovery operations. For example, disaster service workers can be recalled to assist with EOC operations during a disaster.

Figure 6: Effective Emergency Operations Center Characteristics

EOC Information

The Emergency Operations Center maintains key incident information, including the EOC activation level, personnel list, task tracker (current and past), key information/event/decision log, stakeholder list, point of contact information, jurisdictional maps, State/Federal declarations, and media reporting and inquiries. The EOC is also the entity that usually tracks the status of Community Lifelines for the jurisdiction.

For more information about FEMA Community Lifelines and also the Community Lifelines Toolkit, go to: https://www.fema.gov/emergency-managers/practitioners/lifelines

Emergency Operations Centers combine and summarize incident information, including:

- Situation data
- System information flow status
- Communication system integration
- Events log
- Regional weather impact information
- Conflict resolution status
- Jurisdictional resource and aid requests
- State/Federal request status
- Regional maps
- Media reporting and inquiries

Departmental/Business Operations Center

Not every Operations Center meets the NIMS definition of an Emergency Operations Center. Where EOCs are centers for multi-agency, multi-jurisdiction coordination, Departmental, and Business Operation Centers focus on coordinating information and support for their own authorities and responsibilities and the operations of a single department or business. They are a single department, agency, or organization, typically operating within a single jurisdiction coordination (an exception to this is a business operations center for a privately owned business operating in multiple jurisdictions).

Departmental Operations Centers (DOC) function at the agency level (e.g., Police Department, Fire Department, Public Works Department) to support the agency and ensure continuity of service during a significant incident. The DOC is not usually a part of the direct multi-agency coordination for incident response.

Examples of DOC responsibilities include:

- Recalling or hiring off-duty personnel to provide essential staffing
- Placing reserve fleet in service
- Providing supplies and other resources
- Coordinating with mutual-aid agencies to provide coverage/service to the community

The DOC can have a role as a supporting operations center for an incident by providing direction and guidance to field supervisors and personnel from that department or agency that is supporting an incident. They also may have a role in the collection, evaluation, and dissemination of operational information related to the incident for their department or agency. It is important to note that in ICS, there is a Chain of Command and Unity of Command. Every individual dispatched to the incident will operate within a defined Chain of Command and only report to a single supervisor within the ICS organization. Any coordination by an off-scene DOC for their personnel dispatched to the incident cannot interfere with the Chain of Command and Unity of Command on the incident. Departmental Operations Centers tend to focus solely on operations involving that one governmental entity.

Business Operations Centers (BOC) provide similar business-centric coordination for a private sector business. Business Operations Centers perform a similar function for an industry where the need for internal collaboration is required to address a specific issue or impact. Again, they may engage in the direction of resources dispatched to the incident that would not violate the Chain of Command and Unity of Command and support more localized efforts. Examples would be larger corporations, such as big-box retailers utilizing their BOC to move resources in response to a hurricane.

DOC/BOC responsibilities:

- Coordinating emergency response activities within the jurisdiction of the department, agency, or business
- Obtaining intelligence and forecasting potential needs for the department, agency, or business
- Providing logistical support for field personnel of the department or business
- Establishing a chronological reporting system for all incidents and responses
- Summarizing the status of the current department or business operations

Multiagency Coordination Groups

A Multiagency Coordination Group (MAC Group), also referred to as a Policy Group, typically consists of agency administrators or executives from organizations or their designees. They 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. They provide this guidance and direction to the EOC and the Incident Command/Unified Command.

MAC Groups exist at all levels of government: national, regional, and local. They provide an essential management mechanism for strategic coordination to ensure incident resources are efficiently and appropriately managed cost-effectively. They are primarily responsible for resource prioritization and allocation.

The MAC Groups do not perform incident command functions; incident command is the delegated responsibility of the Incident Commander or Unified Command. They also do not replace the primary functions of operations, coordination, or dispatch organizations such as EOCs, DOCs, BOCs, JICs, and dispatch centers. A MAC Group is not typically engaged in activities such as consolidating and exchanging information, supporting decision-making, coordinating resources, and communicating with personnel on the scene.

A MAC Group may require administrative and/or logistical support. In some instances, staff in the EOC provide this support. In other instances, a separate organization may be established to support the MAC Group in meeting its logistical and documentation needs. (NIMS, 2017)

Figure 7: Multiagency Coordination Group Functions

MAC Group Information

The MAC Group normally makes policy decisions in cases where current policy is non-existent or inadequately relates to an issue or challenge encountered during incident response. If a policy is in place and is sufficient, there is no need for policy direction from the MAC Group. The MAC Group makes resource allocation decisions in cases where hard choices have to be made about resource allocation. Again, if there are adequate resources and funding for the incident response, there is no need for the MAC Group to make resource allocation decisions.

To support incident-related policy guidance and scarce resource allocation decisions, the MAC Group requires decision-support information. Decision-support information is the information required by leaders to make an informed decision. This may be provided by the EOC or by a special staff established to support the MAC Group.

Examples of decision-support information that may be required by the MAC Group include:

- Current incident situation
- Projected incident direction (is it stabilizing or getting more complex?)
- Investigative information
- Status of critical or scarce resources
- Current and projected rate of resource and funding utilization
- Identified policy gaps affecting the incident response
- Information requests from the news media and the public (NIMS, 2017)

Joint Information Center and System

The Joint Information System (JIS) is not just Public Affairs; it also includes incident information. JIS integrates both incident information and public affairs efforts to provide consistent, coordinated, accurate, accessible, timely, and complete information to:

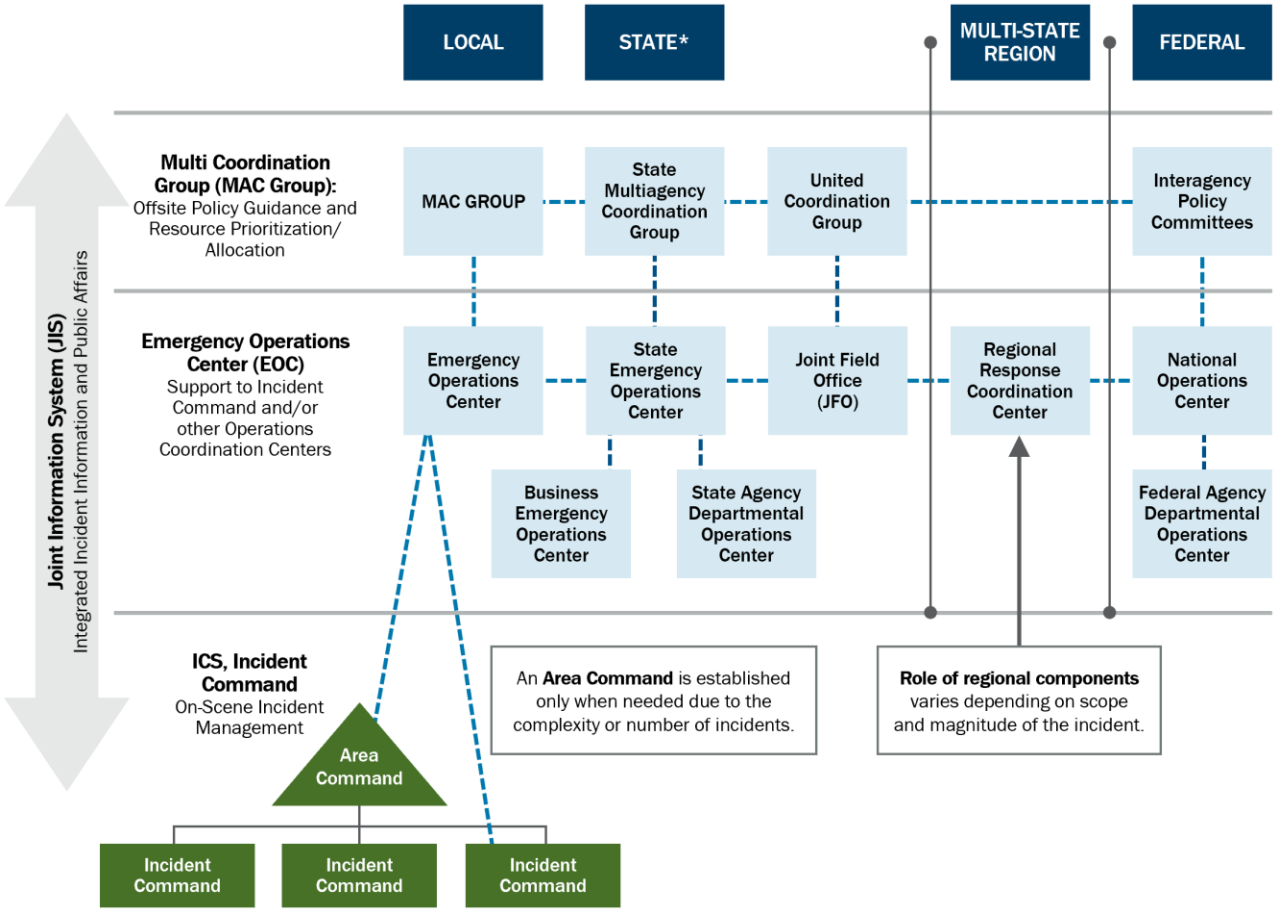
- Incident personnel (ICS, EOC, MAC Group)
- Media
- The public
- Stakeholders

The JIS is not a place; it is the processes, procedures, and tools that enable coordinated communication with incident personnel, the public, the media, and other stakeholders. All the integrated information within the JIS is not provided to everyone. JIS disseminates information to various audiences based on their identified information needs. The MAC Group needs information to make policy and resource decisions, which may be different from the information needed by the Incident Command to manage the incident or by the public to help them understand the situation. Some information is shared widely, while other information may be limited to only audiences with a need to know.

A Joint Information Center (JIC) is different from the JIS. 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 the release of conflicting information, and prevent adverse impacts 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 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.

Figure 8: Command and Coordination in a Large Incident



*Note that some states organize regional or geographical areas to coordinate state-level incident response.

Chapter 2: The Incident Command Staff

Incident response organizations are structured and operate based on the Incident Command System (ICS). An ICS organization is composed of ICS-trained personnel filling ICS positions, including an Incident Commander, Command and General Staff (C&GS), and personnel assigned to other key ICS positions.

The ICS organizational structure can be used to respond to and manage any type of disaster or incident. In this document, "incident" includes planned events as well as emergencies and disasters of all kinds and sizes. The ICS organization includes qualified Operations Section personnel, Technical Specialists, and Safety Officers appropriate for the type of incident (e.g., response and/or recovery for a tornado, flood, civil unrest, public health emergency, hazardous materials release, wildland fire). The support components of the ICS organization (e.g., Planning Section, Logistics Section, Finance Section, Command Staff, and units) complement and support the operational response and recovery effort by utilizing a standardized approach based on the Incident Command System (ICS) and the National Incident Management System (NIMS).

As incidents expand, the ICS organization can also expand as necessary for the type, size, scope, and complexity of the incident. The ICS organization builds from the top down. When needed, Sections can be added to this organization, and each Section may have further subordinate units. This modular concept is based on the following considerations:

- The organization matches the function or task to be performed and the Resources that must be managed to perform these tasks and functions
- Staffing is made only for those functional elements required to perform the task
- Span of control guidelines are maintained
- The function of any non-activated organizational element is performed at the next highest level
- Organizational elements are deactivated if they are no longer required

Not all incident command organizations are called Incident Management Teams (IMTs). An incident command is only referred to as an IMT when it has all the following characteristics:

- A rostered group composed of ICS-qualified personnel
- Configured using the ICS organizational structure
- Includes an Incident Commander, command and general staff members, and support personnel
- Has statutory authority and/or formal response requirements and responsibilities
- Has pre-designated roles and responsibilities for members (identified and able to be contacted for deployment)
- Members are trained, qualified, and credentialed to perform their pre-designated roles

- Are available based on a pre-established schedule (24/7/365, seasonal, or rotational)
- The level of training and experience of the ICS-qualified personnel, coupled with the identified formal response requirements and responsibilities of the ICS organization, are factors in determining the "type," or level, of IMT

ICS Position Training courses and this Reference Guide are not intended for IMTs only. They are broadly applicable to all ICS organizations. The course materials contain information derived from the guidance and best practices of experienced ICS practitioners, including IMTs, the wildland firefighting community, and the U.S. Coast Guard.

Types of ICS Organizations

Standing ICS Organizations

Standing teams are those ICS organizations that are pre-established, rostered, have routine meetings and training courses, and typically have written procedures already in place for their members. These are commonly referred to as Incident Management Teams (IMTs). IMTs are generally typed and classified according to their capability. A Type 1 Team is considered to be more capable than Types 2, 3, or 4 due to their experience and qualifications.

Ad Hoc Teams

Ad hoc teams are those teams that are typically not pre-designed or rostered and are comprised of members who may or may not regularly work together but are assigned to the standardized ICS roles in a situation. Members of Ad Hoc ICS organizations often have formal qualifications and certifications from their Authorities Having Jurisdiction to perform an incident-specific role.

Role of the IMT: Supporting Effective Response and Recovery

Again, not all incident command organizations are Incident Management Teams (IMTs). An IMT is a comprehensive resource to either:

- Augment and support ongoing response/recovery efforts by providing additional trained staff capable of filling ICS positions within an Incident Command/Unified Command
- Transition to an incident management role, which includes performing all components and functions of the Incident Commander and Command and General Staff

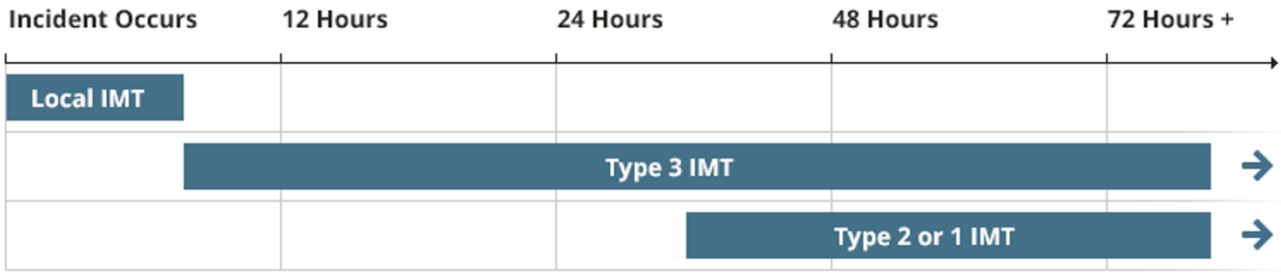
IMTs exist to assist with events and incidents that:

- Exceed the capacity of local resources
- Require special expertise to manage only certain parts of an incident, such as planning, logistics, or finance, which, in turn, allow local responders to remain focused on operations

IMTs can also support when assistance is needed for recovery activities rather than response. Many communities may have experience with response, but little in the way of formal recovery efforts. It is worth noting that deploying partial IMTs to assist in events such as these is now quite common. In some cases, IMTs may augment incident support efforts by providing trained staff capable of filling positions within an EOC.

A timeline showing the typical timeframes for response and operations of the different "Types" of IMTs is shown in Figure 9.

Figure 9: Typical Timeframes for Response and Operations



Incidents are usually first managed by the local incident command, which may be a locally organized IMT. For more complex incidents, the local IMT may be replaced by more capable Type 3, 2, or 1 IMTs.

Common Responsibilities of All ICS Members

ICS staff are trained, qualified, and credentialed in specific jobs and functions. Each specific ICS position is assigned tasks related to the function they perform within the Incident Command. Additionally, there are several common tasks that all ICS personnel perform, regardless of their position.

Listed below are responsibilities that are usually applicable to all ICS personnel. These responsibilities are described in much greater depth in Chapter 3.

- Have your "Go-Kits" stocked, ready, and checked before you leave. A Go-Kit includes the equipment and supplies that you will need for your initial response.
- Receive your assignment from your agency, including job assignment, resource order number, request number, reporting location, time, incident contact information, travel instructions, and any special communications instructions.

- Research and learn about the area, event, and community.
- Upon arrival at the incident, check in at the designated Check-in location. They may use an electronic system or an Incident Check-in List (ICS Form 211).
- Receive briefing from immediate supervisor.
- Acquire work materials.
- Conduct all tasks in a manner that ensures the safety and welfare of you and your co-workers by utilizing accepted risk analysis methods.
- Follow the designated process for ordering resources and materials.
- Organize and brief subordinates.
- Know the assigned frequency or frequencies for your area of responsibility and ensure that communication equipment is operating properly.
- Use clear text and NIMS terminology (no codes) in all communications.
- Complete forms and reports required of the assigned position and send them through the supervisor to Documentation Unit.
- Maintain an Activity Log (ICS Form 214).
- Respond to demobilization orders and brief subordinates regarding demobilization.

Common Responsibilities of All ICS Leaders

A number of the responsibilities that are common to all leaders in all parts of the organization are listed below. These are described in greater detail in Chapter 3.

- Communicate Leaders Intent
- Assign and Track Tasks
- Participate in Meetings and Briefings
- Promote Situational Awareness and Common Operating Picture
- Manage Information and Documentation
- Promote Safety and Security
- Lead Assigned Staff
- Manage Assigned Resources

ICS Position Responsibilities

All personnel must execute their responsibilities following established guidelines for effective and safe incident management. Personnel are deployed to an incident at the request of the appropriate authority. Individuals remain deployment-ready by maintaining the skills, knowledge, certifications, physical fitness, equipment, and any other items required or recommended by their organization.

Area Commanders/Unified Area Command

Responsible for the overall direction of all incidents assigned to the Area Command/Unified Area Command by the Authority Having Jurisdiction. This responsibility includes ensuring that conflicts are resolved, incident objectives are established, and strategies that ensure the best use of scarce resources 7are selected. The Area Commander/Unified Area Commander coordinates with local, state, tribal, territorial, and federal departments and agencies, as well as NGOs and other private sector elements, in establishing priorities for all incidents in Area Command/Unified Area Command. When an Area Command/Unified Area Command is established, all the assigned Incident Commanders report to the Area Commander/Unified Area Commander.

Incident Commander/Unified Command

The Incident Commander/Unified Command is not a part of either the General or Command Staff. The Incident Commander/Unified Command manages the incident through the Command and General Staff.

The Incident Commander/Unified Command is responsible for:

- Knowing agency policy
- Ensuring clear authority derived from jurisdictional policy or delegated authority to act
- Having clear authority and knowing agency policy
- Ensuring incident safety
- Establishing an Incident Command Post
- Establishing leader's intent and priorities
- Determining incident objectives and strategies
- Establishing the ICS organization needed to manage the incident
- Approving the Incident Action Plan and Demobilization Plan
- Coordinating Command and General Staff activities
- Approving resource requests and use of volunteers and auxiliary personnel
- Ensuring after-action reports are completed
- Authorizing Public Information Officer to release information to the media (in coordination with the EOC Public Information efforts and based on the MAC Group's guidance and policy direction)
- Ordering demobilization of resources as needed

Deputies

The Incident Commander may have one or more Deputies. An individual assuming a Deputy role must be equally capable of assuming the primary role. A Deputy Incident Commander must meet the same qualifications and be able to fully perform the Incident Commander's role.

The following are some of the reasons an Incident Commander might designate Deputies:

- To perform specific tasks requested by the Incident Commander
- To perform the Incident Command function in a relief capacity (e.g., to take over the next Operational Period)
- To represent an assisting agency that may share jurisdiction or have jurisdiction in the future
- To focus on special or advanced planning efforts beyond the next operational period

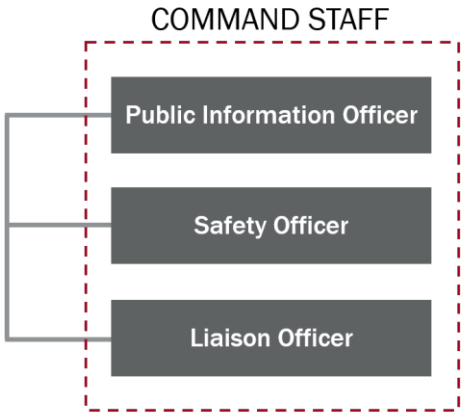
The Operations Section Chief, Planning Section Chief, Logistics Section Chief, Finance/Administration Section Chief, and Branch Directors may also have one or more Deputies.

Command Advisors

The Incident Commander or Unified Command may appoint technical specialists to serve as command advisors. Command Staff advisors differ from Command Staff Officers (Public Information, Safety, Liaison) in that they serve in advisory capacities and lack the authority to direct incident activities.

Command Staff

Figure 10: ICS Command Staff Positions



The Command Staff is assigned to carry out staff functions needed to support the Incident Commander. These functions include public information, safety, and interagency liaison.

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

One of the organizational options for the Intelligence/Investigations function is to place it within the Command Staff.

Public Information Officer

The Public Information Officer interfaces with the public, media, and/or other agencies with incident-related information needs. The Public Information Officer gathers, verifies, coordinates, and disseminates accessible, meaningful, and timely information on the incident to both internal and external audiences.

The Public Information Officer also monitors the media and other sources of public information. They collect relevant information and transmit it to the appropriate segments of the incident management organization. In incidents that involve Public Information Officers from different agencies, the Incident Commander or Unified Command designates one as the lead Public Information Officer. All Public Information Officers should work in a unified manner, speak in one voice, and ensure that all messaging is consistent. Information efforts must be coordinated across all command and coordination entities, not just within the incident command. The Public Information Officer does not have independent authority to release information. The Incident Commander or Unified Command approves the release of incident-related information based on the guidance and direction they have been given by the Agency Administrator or the MAC Group.

In large-scale incidents where a Joint Information Center is established, the Public Information Officer participates in or leads the Joint Information Center (JIC). The Public Information Officer may have assistants (not deputies).
Other Public Information Officer duties include:

- Determining any restrictions on information release according to direction from the Incident Commander based on the guidance and direction of the Agency Administrator
- Obtaining the Incident Commander's approval of news releases (again, the Incident Commander approves information released based on the guidance and direction of the Agency Administrator)
- Conducting periodic media briefings
- Arranging tours and other interviews or briefings that may be required

- Maintaining current information, summaries, and/or displays on the incident
- Making information about the incident available to incident personnel
- Participating in planning meetings
- Organizing, participating in, and leading public meetings

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. They report to the Incident Commander or Unified Command and are responsible for establishing the systems and procedures necessary to assess, communicate, and mitigate hazardous environments. The Safety Officer participates in the preparation of the tactical plan for the next operational period by attending the Tactics Meeting and completing an Incident Safety Analysis (ICS Form 215A). The Safety Officer shall be knowledgeable in the operations being implemented at the Emergency Response site (scene), identify and evaluate hazards, and provide direction with respect to the safety of operations for the emergency at hand.

This includes developing and maintaining the Safety Message/Plan (ICS Form 208), coordinating multiagency safety efforts, and implementing measures to promote the safety of incident personnel and incident sites. Per 29 CFR, in hazardous material incidents, the Safety Officer shall have the authority to alter, suspend, or terminate activities for situations judged to be an immediate danger to life & health (IDLH). The Safety Officer stops and/or prevents unsafe acts by providing safety guidance to the ICS organization as well as personally monitoring incident activities for safety. Agencies, organizations, or jurisdictions that contribute to joint safety management efforts do not lose their responsibilities or authority for their own programs, policies, and personnel. Rather, each contributes to the overall effort to protect all personnel involved in the incident. Ensuring safety is the responsibility of all incident personnel. The Safety Officer may have assistants (not deputies).

Other Safety Officer duties include:

- Ensuring that safety messages are published and briefings are conducted
- Exercising emergency authority to stop and prevent unsafe acts
- Reviewing the Incident Action Plan for potential safety and occupational health implications
- Assigning assistants qualified to evaluate special hazards
- Initiating preliminary investigation of accidents within the incident area
- Reviewing, signing, and approving the Medical Plan (ICS Form 206)

- Participating in the planning process including the tactics and planning meetings and the Operations brief

Liaison Officer

Under either an Incident Commander or a Unified Command, representatives from assisting or cooperating jurisdictions and organizations coordinate through the 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 Incident Command or Unified Command. These representatives provide input on their agency, organization, or jurisdiction's policies, resource availability, and other incident-related matters through the Liaison Officer. The Liaison Officer may have assistants (not deputies).

Other Liaison Officer duties include:

- Assisting in setting up and coordinating interagency contacts
- Monitoring incident operations to identify current or potential inter-organizational problems
- Participating in planning meetings, providing current resource status, including limitations and capabilities of agency resources
- Providing agency-specific demobilization information and requirements
- Organizing, participating in, and leading cooperator meetings

Agency Representatives

An Agency Representative is an individual assigned to an incident by an assisting or cooperating agency. The Agency Representative must be given authority to make decisions on matters affecting that agency's participation in the incident. Agency Representatives are not a formal part of the ICS organization but are there to represent agencies with resources deployed to the incident. Agency Representatives report to the Liaison Officer or the Incident Commander (in the absence of a Liaison Officer).

Major responsibilities of an Agency Representative include:

- Ensuring that all of their agency resources have been checked in at the incident
- Obtaining briefings from the Liaison Officer or Incident Commander
- Informing their agency personnel on the incident that the Agency Representative was briefed on
- Attending planning meetings as required

- Providing input to the planning process on the use of agency resources unless resource Technical Specialists are assigned from the agency
- Cooperating with the Incident Commander and the Command and General Staff on the agency's involvement in the incident
- Overseeing the well-being and safety of agency personnel assigned to the incident
- Informing the Liaison Officer of any special agency needs, requirements, or agency restrictions
- Reporting to agency dispatch or headquarters on a prearranged schedule
- Ensuring that all agency personnel and equipment are properly accounted for and released prior to departure
- Ensuring that all required agency forms, reports, and documents are complete prior to departure
- Debriefing with the Liaison Officer or Incident Commander prior to departure

Assistants

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

The Public Information Officer, Safety Officer, and Liaison Officer may have Assistants as necessary. The Assistants may assist agencies or jurisdictions or simply assist in managing the workload associated with the position.

Assistant Public Information Officers may be assigned to the field or Joint Information Center or assigned to handle internal information.

Assistant Safety Officers may have specific responsibilities, such as aviation, hazardous materials, etc.

Assistant Liaison Officers may coordinate with specific agency representatives or groups of representatives.

The Assistant title indicates a level of technical capability, qualification, and responsibility subordinate to the primary positions.

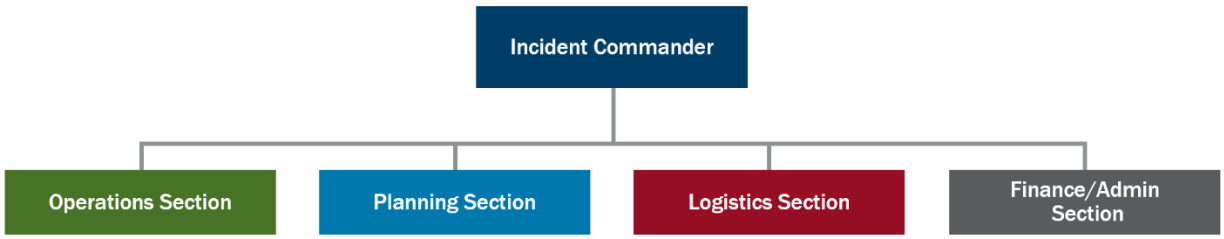
Additional Staff

Depending on the nature and location(s) of the incident, as well as any unique criteria established by the Incident Commander, additional positions may be required to support the Incident Command/Unified Command. In 2017, NIMS established the position of “command advisor.” For example, a Legal Advisor may be assigned directly to the Command Staff to advise the Incident Commander on legal matters, such as emergency proclamations, legality

of evacuation orders, and legal rights and restrictions on media access. Similarly, a Medical Advisor may be designated and assigned directly to the Command Staff to provide advice and recommendations to the Incident Commander on matters involving medical and mental health services, mass casualty, acute care, vector control, epidemiology, and/or mass prophylaxis considerations, particularly in response to a bioterrorism event. These positions may also be referred to as Technical Specialists (THSP) assigned to the Incident Command/Unified Command.

General Staff

Figure 11: ICS General Staff Positions



The ICS General Staff is responsible for the functional aspects of the Incident Command structure. The General Staff typically consists of the Operations, Planning, Logistics, and Finance/Administration Sections. In some incidents, the General Staff may also include an Intelligence/Investigations Section if there is a significant Intelligence/Investigations effort.

When thinking about what Sections may be activated in a response, remember the NIMS Management Characteristics Modular Organization and Manageable Span of Control. The ICS organizational structure develops in a modular fashion based on the size, complexity, and hazard environment. A key consideration is having an adequate structure to maintain a manageable span of control. More resources generally require more ICS organizational structure to maintain the span of control. When a Section or a subordinate element is not established in the ICS organizational structure, the functions performed by that element are performed by the next higher supervisory position. This continues until that supervisor delegates that function to a subordinate position.

General guidelines related to General Staff positions include the following:

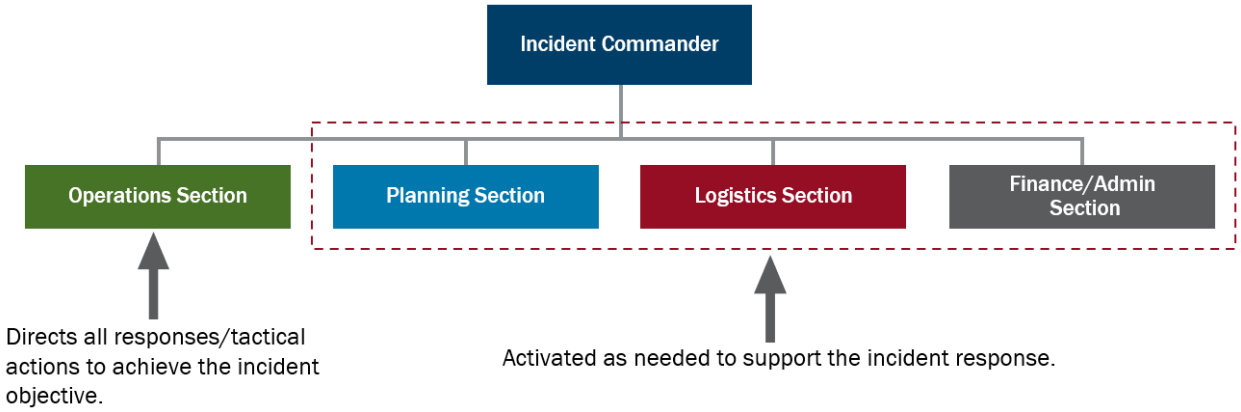
- Only one person will be designated to lead each General Staff position.
- General Staff positions may be filled by qualified persons from any agency or jurisdiction.
- Members of the General Staff report directly to the Incident Commander. If a General Staff position is not activated, the Incident Commander will take responsibility for that functional activity.

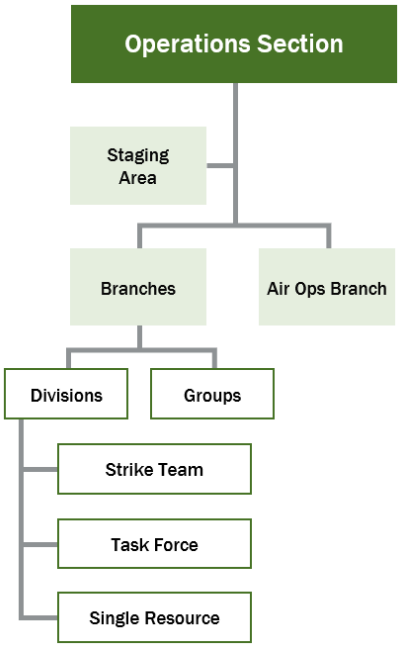
- Deputy positions may be established for each of the General Staff positions. Deputies are individuals fully qualified to fill the primary position. Deputies can be designated from other jurisdictions or agencies if appropriate. This is a good way to bring about greater interagency coordination.
- General Staff members may exchange information with any person within the organization. Direction takes place through the chain of command. This is an important concept in ICS.
- General Staff positions should not be combined. For example, to establish a "Planning and Logistics Section," it is better to initially create two separate functions and, if necessary for a short time, place one person in charge of both. That way, the transfer of responsibility can be made easier.
- If the incident organization is small and General Staff positions have not been filled, then the Incident Commander will personally request additional resources from the agency dispatch/ordering center.

Operations Section

Operations Section staff are responsible for tactical activities that typically focus on saving lives, reducing immediate hazards, 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.

Figure 12: ICS Operations Section Positions





Operations Section Chief (OSC)

The Operations Section Chief is responsible for managing all tactical operations during an incident, and the Incident Action Plan (IAP) provides the necessary guidance. The need to expand the Operations Section (e.g., activate branches or divisions and/or groups) is dictated by the number of tactical resources involved and is influenced by the span of control considerations.

Major responsibilities of the Operations Section Chief are:

- Assure the safety of tactical operations
- Manage tactical operations
- Develop primary and alternate strategies, tactics, and contingency plans for the incident
- Plan for the next operational period
- Develop the operations portion of the Incident Action Plan
- Supervise the execution of operations portions of the Incident Action Plan
- Request additional resources to support tactical operations
- Approve the release of resources from active operational assignments
- Make or approve expedient changes to the Incident Action Plan

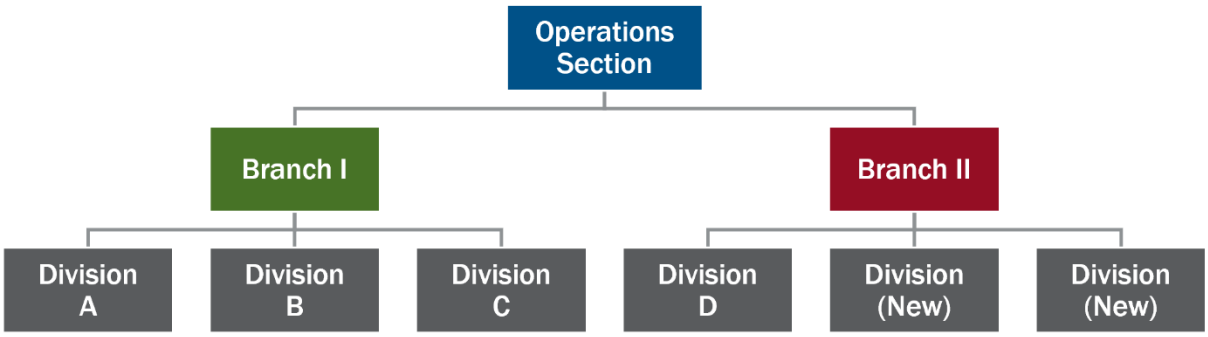
- Maintain close contact with Incident Commander, subordinate Operations personnel, other Command and General Staff members, and other agencies involved in the incident

Branch Directors

Branch directors are inserted between the Operations Section Chief and the divisions and/or groups when the number of divisions and/or groups exceeds a manageable span of control or when critical functions must be handled independently within the Operations Section. Branch Directors manage divisions or groups and report directly to the Operations Section Chief. Each Branch Director is responsible for implementing the portion of the Incident Action Plan (IAP) applicable to their assigned Branch and managing significant geographical and/or functional portions of the incident assigned to them.

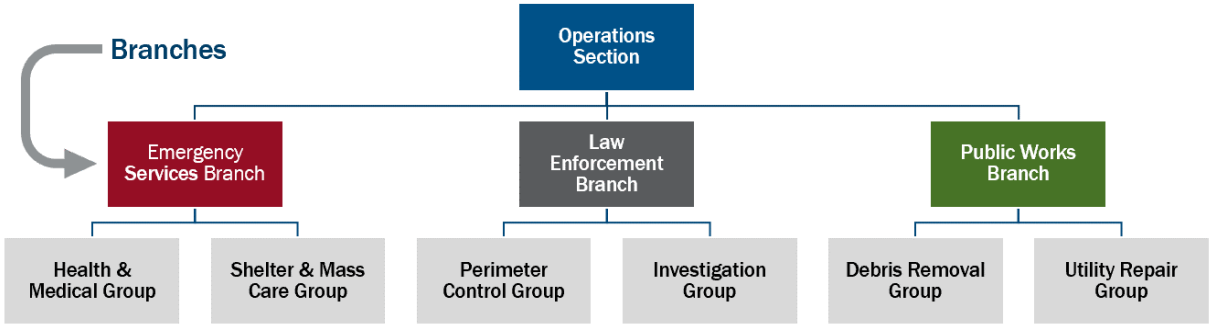
Branches may be established to manage two or more divisions and/or groups within a defined geographic boundary. Within this geographic boundary, there can be a variety of sources performing diverse functions, such as law enforcement, fire suppression, or emergency services. Geographic branch boundaries are depicted on incident maps and clearly communicated to incident personnel.

Figure 13: ICS Operations Section Use of Geographic Branches



Branches may also be established functionally. When this is done, the Branch Director will be responsible for a single specific function such as law enforcement, fire suppression, or emergency services. All subordinates working for a functionally organized branch will be responsible for all assigned functions within the branch area of responsibility. (NIMS, 2017)

Figure 14: ICS Operations Section Use of Functional Branches



Branches also are used by other ICS Sections outside of the Operations Section. We will discuss these later.

Major responsibilities of the Branch Director are:

- Identify Division/Group boundaries and staging
- Name/order required branch resources
- Communicate priorities, tactics, and changes to Branch personnel
- Have processes for resource requests and releases
- Anticipate mid and long-range resource and logs needs
- Review Incident Action Plan for effectiveness
- Give Branch status updates and needs for the next operational period to the Operations Section Chief
- Evaluate the current situation, resource status, and tactical needs

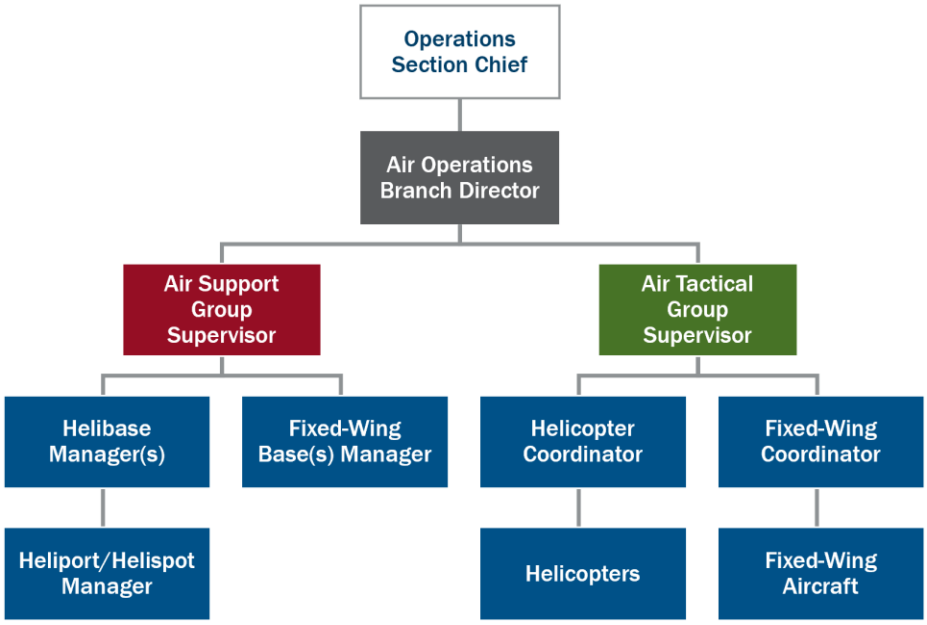
Air Operations Branch Director

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 (e.g., mixed use of helicopters and other aircraft for tactical support), the Operations Section Chief may establish an Air Operations Branch.

Air operations are a high-risk component of the Operations Section, carrying a high potential for severe injury and fatalities. The management of air operations requires highly specialized knowledge and expertise. An Air Operations Branch helps ensure the safe and efficient use of aviation resources.

The Air Operations Branch Director reports to the Operations Section Chief and is primarily responsible for preparing the air operations portion of the IAP, implementing its strategic aspects, and providing logistical support to aircraft operating on the incident.

Figure 15: ICS Operations Section Air Operations Branch



The Air Operations Branch Director's functions are:

- Supervise Air Branch Operations
- Indicate/assign Air Support Group Supervisor and Air Tactical Group Supervisor
- Manage/coordinate air ops activities
- Provide intelligence and feedback to Operations Section Chief
- Look for the need to plan for contingencies
- Implement pilot and aircraft hours tracking system
- Fill out appropriate documentation (ICS Form 220)
- Indicate/solve all Air Branch problems
- Evaluate the effectiveness of air operations and report any unsafe situations/issues
- Sit in on all the needed Planning and Operation meetings

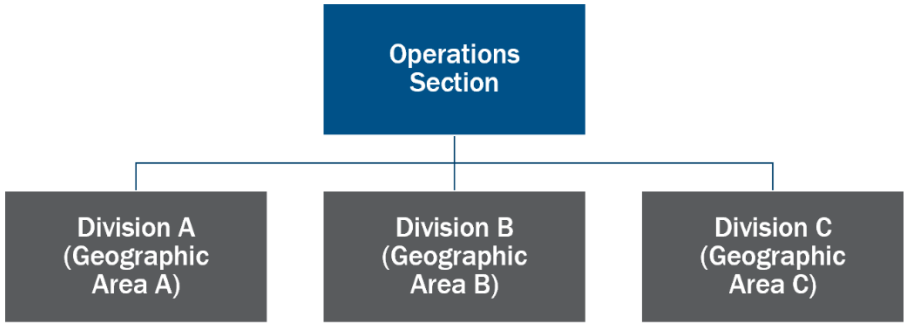
Division/Group Supervisors

The Operations Section Chief establishes divisions and groups when the number of resources exceeds a manageable span of control. The use of the word division refers to geographic assignments, and the use of the word group refers to functional assignments. Both divisions and groups may be used in a single incident.

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.

Division Supervisors manage tactical operations and supervise resources (e.g., task forces, strike teams, crews/teams, single resource) in their assigned geographical area in accordance with the IAP. Divisions are designated by capital letters (e.g., DIV-A, DIV-C). (NIMS, 2017)

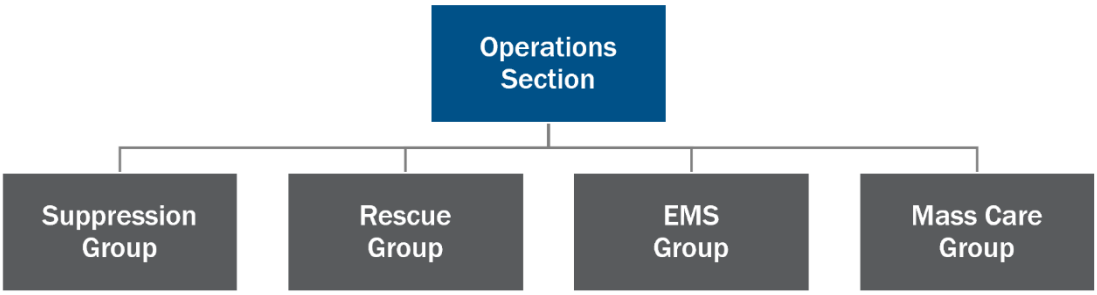
Figure 16: Operations Section Use of Geographical Divisions



Groups are used to describe similar functional areas of activity (e.g., rescue, evacuation, law enforcement, medical treatment, or triage).

Group Supervisors manage tactical operations and supervise resources (e.g., task forces, strike teams, crews/teams, single resources) in specific functional assignments (e.g., Hazmat Group, Perimeter Control Group, Debris Removal Group) in accordance with the IAP. Division and Group Supervisors report to a branch director if activated or directly to the Operations Section Chief if no branch is activated.

Figure 17: Operations Section Use of Functional Groups



The specific functions of Division and Group Supervisors are:

- Provide IAP information to Strike Team/Task Force personnel
- Implement IAP for Division/Group
- Translate Operations Section Chief directives into tactical operations
- Coordinate activities with adjacent Divisions/Groups
- Review assignments and tasks with personnel
- Evaluate/determine the need for additional resources

- Work on/submit SITSTAT info to Branch or Operations Section Chief
- Solve Division/Group logistical problems (NIMS, 2017)

Air Support Group Supervisor

Air Support Group staff create and operate helicopter bases, as well as maintain contact with off-incident fixed-wing bases.

The Air Support Group Supervisor is primarily responsible for operating all Helibase and Helispot operations and fixed-wing air bases assigned to the incident.

This includes providing:

- Fuel and other supplies
- Maintenance and repair of helicopters
- Fire retardant mixing and loading
- Keeping records of helicopter activity
- Providing enforcement of safety regulations

These major functions are performed at Helibases, Helispots, and fixed-wing air bases. Aircrafts assigned to the incident are under the control of the Air Support Group's Helibase Manager or Fixed Wing Base Manager during landing, takeoff, and while on the ground. Although the Logistics Section Chief is responsible for providing for the incident support needs, the Air Support Group, rather than the Logistics Section, provides aviation-specific logistical support for air operations. There are a relatively small number of qualified Air Operations Branch Directors outside of wildland firefighting. Many response operations involving aviation resources operate with Air Support and/or Tactical Group Supervisor without an Air Operations Branch Director. In these cases, the Group Supervisors report directly to the Operations Section Chief. (USFA NFA, 2016)

The Air Support Group Supervisor is responsible for:

- Obtaining a copy of the Incident Action Plan, including Air Operations Summary (ICS Form 220)
- Participating in Air Operations Branch Director planning activities
- Tracking flight and duty hours
- Informing Air Operations Branch Director of group activities
- Identifying resources/supplies dispatched for Air Support Group
- Requesting special air support items from appropriate sources through Logistics Section
- Identifying Helibase and Helispot locations (from Incident Action Plan or Air Operations Branch Director)
- Determining the need for assignment of personnel and equipment at each Helibase, Helispot, and Fixed Wing Bases
- Coordinating special requests for air logistics

- Maintaining coordination with airbases that are supporting the incident
- Coordinating activities with Air Operations Branch Director
- Obtaining assigned ground-to-air frequency for Helibase operations from Communications Unit Leader or Incident Radio Communications Plan (ICS Form 205)
- Informing the Air Operations Branch Director of the capability to provide night-flying service
- Ensuring compliance with each agency's operations checklist for day and night operations
- Ensuring dust abatement procedures are implemented at Helibase and Helispots
- Providing aircraft rescue firefighting service for Helibases, Helispots, and Fixed Wing Bases, when needed
- Ensuring that Air Traffic Control protocols and flight following requirements are established in Helibase, Helispots, and Fixed Wing Bases

Air Tactical Group Supervisor

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. The Air Tactical Group Supervisor performs these coordination activities while airborne.

The Air Tactical Group Supervisor is responsible for:

- Determining what aircraft are operating within the area of assignment (can include fixed wing, air tankers, aerial cargo delivery, smokejumpers, helicopters, and UAVs) Managing air tactical activities based upon Incident Action Plan
- Determining the need and size of a Temporary Flight Restriction (TFR) and making the request
- Establishing and maintaining communications with pilots and Air Traffic Control, Helicopter Coordinator, Air Tanker/Fixed Wing Coordinator, UAS Coordinator, Air Support Group Supervisor (often a Helibase Manager), and fixed-wing bases. Coordinating approved flights of non-incident aircraft or non-tactical flights in the restricted air space area
- Managing assigned small Unmanned Aircraft Systems (sUAS) within operations as a part of overall air tactical operations
- Obtaining information regarding air traffic that is not related to the incident
- Receiving reports of non-incident aircraft violating restricted air space areas
- Making tactical recommendations to approved ground contact (Operations Section Chief, Operations Branch Director, or Division/Group Supervisor)
- Informing the Air Operations Branch Director of tactical recommendations affecting the air operations portion of the Incident Action Plan

- Reporting the Air Operations activities to the Air Operations Branch Director
- Advising Air Operations immediately if aircraft mission assignments are causing conflicts in the Air Traffic Control System
- Reporting on incidents/accidents
- Updating the Air Operations Branch Director or Operations Section Chief on the effectiveness of Air Operations and making recommendations to adjust strategies
- Monitoring weather conditions that could impact Air operations

Staging Area Manager

Staging Areas are locations for gathering resources that are assigned to the incident but awaiting tactical assignment. These resources must maintain the ability to respond. If a resource is not available for tactical assignment, it does not belong in Staging.

In an incident, staged resources may be used as part of a Contingency Plan to initially respond to new incidents, relieve assigned resources, or be assigned as additional resources. Resources that are released from a particular operational assignment may be reassigned to the Staging Area while it is determined whether they will be reassigned or declared as excess.

A Staging Area Manager manages the physical area and resources temporarily assigned to the staging area. These resources are a tactical reserve for the Operations Section.

The Staging Area Manager:

- Keeps an inventory of the staging area
- Acts as a point of contact with the Resources Unit in the Incident Command Post (ICP)
- Reports directly to the Operations Section Chief or to Branch Director level supervision when delegated

The Operations Section Chief may establish more than one Staging Area; a separate Staging Area Manager would normally be appointed to manage each Staging Area. Staging areas can be based on functional or geographical requirements, such as hazardous materials staging areas.

Task Force/Strike (Resource) Team Leaders

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

Task forces combine various kinds and types of resources to accomplish a specific mission under a designated leader. They allow a single supervisor to oversee several valuable resource elements. Task Force Leaders manage tactical assignments with dissimilar tactical

resources (e.g., fire engines and police patrol cars, or front-end loaders, dump trucks, and public works crews).

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. In the law enforcement community, strike teams are sometimes referred to as Resource Teams. Strike Team/Resource Team Leaders manage tactical assignments and resources (e.g., patrol cars or medic units).

Task Force/Strike Team Leaders typically report to Division or Group Supervisors and supervise "packaged" resources. Resources could be ordered as a package or assembled at the incident. The Task Force or Strike Team normally operates on a common radio frequency.

Functions of Task Force, Strike team, and Resource Team Leaders:

- Review assignments/responsibilities with personnel
- Assess and monitor work progress
- Coordinate activities with other Task Forces/Strike Teams
- Ensure safe travel to and from the assignment area
- Report work progress and resource status to Division/Group

Single Resource

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

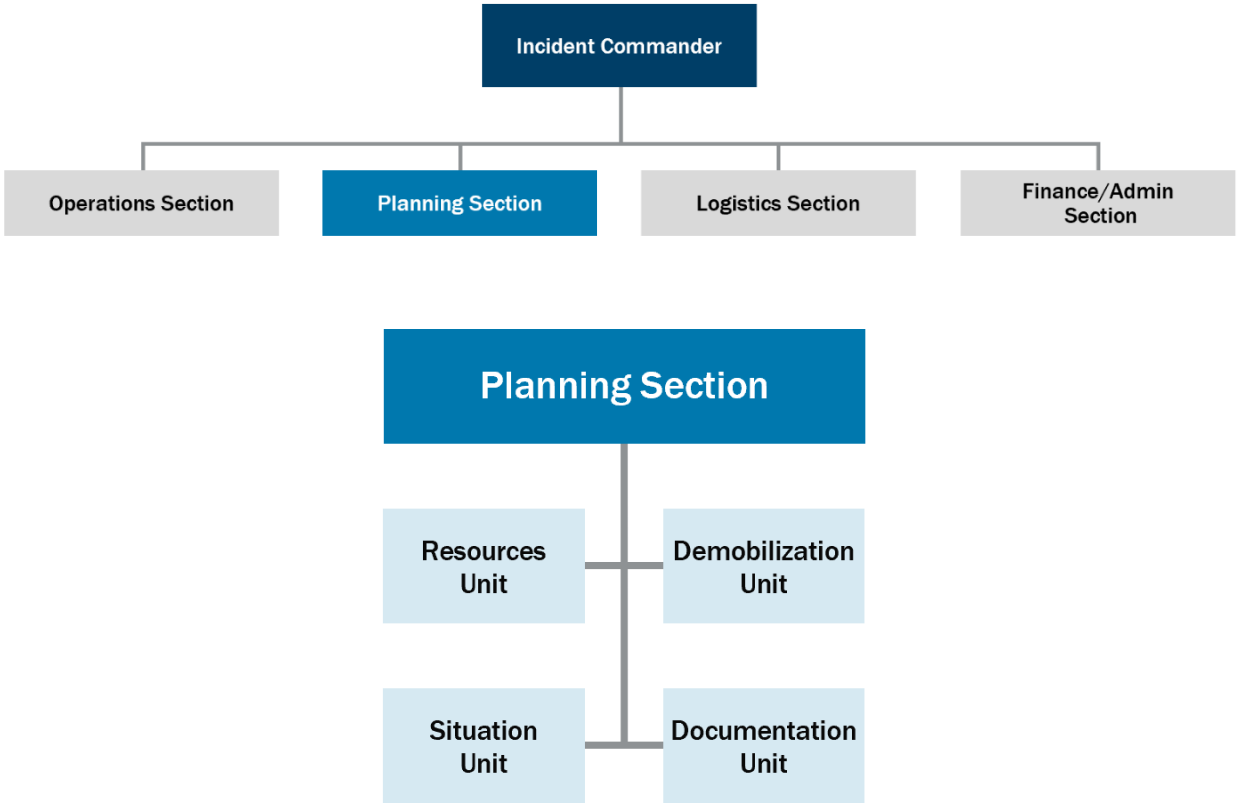
Examples of single resources include an individual patrol car, medic unit, fire engine, front-end loader, specialized teams (e.g., Hazmat, Technical Rescue, Mobile Field Force), or crews (e.g., wildland firefighting, environmental cleanup).

Single resources may be packaged into task forces or strike teams to manage the span of control. During the initial response to an incident, single resources may report directly to the Incident Commander, the Operations Section Chief, or a division or group supervisor. Every single resource has its own supervisor, but the naming convention may be different for each (NIMS guidelines use the terms boss or leader).

Planning Section

The ICS Planning Section collects, evaluates, and disseminates incident information. 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 has four primary units. The Planning Section may also include technical specialists who provide expertise in specific areas and assist in evaluating the situation and forecasting resource requirements.

Figure 18: The Planning Section



Planning Section Chief

The Planning Section Chief oversees incident-related data collection and analysis relating to incident operations and allocated resources, as well as facilitating incident action planning meetings and preparing the IAP for each operational period. This individual is selected based on qualification for the position and may come from the jurisdiction or organization with primary incident responsibility.

The Planning Section Chief is responsible for facilitating and providing support for the incident action planning process. Under the direction of the Planning Section Chief, the Planning Section collects situation and resource status information, evaluates it, and processes the information for use in developing action plans. Dissemination of information can be through a combination of the Incident Action Plan (IAP), formal briefings, maps, and other physical or electronic incident status displays.

Major responsibilities of the Planning Section Chief include:

- Collect and manage all incident-relevant operational data
- Supervise the preparation of the Incident Action Plan

- Provide information to the Incident Commander and Operations during the preparation of the Incident Action Plan
- Incorporate Traffic, Medical, and Communications Plans and other supporting materials into the Incident Action Plan
- Conduct and facilitate most incident action planning meetings Document reassignment of personnel and maintain resource accountability within the ICS organization Compile and display incident status information
- Establish information requirements and reporting schedules for units (e.g., Resources Unit and Situation Unit)
- Determine requirements for specialized resources
- Assemble and disassemble Strike Teams, Task Forces, or Resource teams from single resources as requested by Operations Establish specialized data collection systems as necessary (e.g., weather)
- Assist with/coordinate other types of plans, e.g. contingency, transition, long-range strategic planning
- Assemble information on alternative strategies
- Provide periodic predictions on incident potential
- Report significant changes in incident status
- Oversee preparation of the Demobilization Plan

Situation Unit Leader

The Situation Unit collects, processes, and organizes ongoing situation information; prepares situation summaries; and develops projections and forecasts of events related to the incident. The Situation Unit also prepares maps and gathers and disseminates information (and investigation-related intelligence) for use in the Incident Action Plan document. This unit produces Situation Reports (SITREP) as scheduled or at the request of the Planning Section Chief or Incident Commander.

To perform its role, the Situation Unit may require the expertise of Technical Specialists and Operations and Information Security Specialists. 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.

The Situation Unit leader manages a staff that gathers, analyzes, and disseminates the data needed for Operations and by the other incident personnel.

Responsibilities of the Situation Unit Leader include:

- Collecting, analyzing, processing, organizing, disseminating, and maintaining incident information
- Prepare future projections of incident growth, maps, and essential information

Resources Unit Leader

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

This unit creates a tracking system that displays the resource status of all resources at the incident (Available, Assigned, and Out of Service).

The Resources Unit also maintains a master list of all resources. 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.

Some key responsibilities of the Resources Unit Leader include:

- Retrieve resource status information
- Obtain and track the status of all operational resources
- Create and maintain a list of resources based on information gathered from on-scene incident personnel
- Respond to requests about resource status and location

Note that the Resources Unit tracks resources assigned to an incident, but Logistics Section will provide the most current input on what resources have been ordered and expected in time for the operational period but have not yet checked in.

Documentation Unit Leader

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.

The Documentation Unit Leader ensures that accurate and complete incident files, including a complete record of the major steps taken to resolve the incident, are maintained. The Document Unit files, maintains, and stores incident files for legal, analytical, and historical purposes.

Some key responsibilities of the Documentation Unit Leader include:

- Ensure adequate duplication capability for large-scale operations and adequate staff to assist in the duplication and documentation process
- Establish and organize the Incident File
- Establish duplication services and respond to requests
- Determine the number needed and duplicate Incident Action Plan accordingly
- Retain and file duplicate copies of official forms and reports
- Accept and file reports and forms submitted by incident personnel
- Check the accuracy and completeness of records submitted for files
- Ensure that legal restrictions on public and exempt records are observed
- Provide briefing on current activities and briefing to create relief in unusual events
- Give completed incident files to the Planning Section Chief

Demobilization Unit Leader

Demobilization Unit staff develop an Incident Demobilization Plan, which includes specific instructions for all personnel and other resources to be demobilized. They begin their work early in the incident, and their job includes 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.

The Demobilization Unit Leader develops an Incident Demobilization Plan, which includes specific instructions for all personnel and resources that will require demobilization. The Demobilization Unit Leader assists the Command and General Staff in ensuring an orderly, safe, and efficient movement of personnel and equipment from the incident.

Demobilization Unit Leader responsibilities include:

- Monitoring the status of resources
- Reviewing incident resource records
- Identifying surplus resources
- Notifying resources of their demobilization date and time
- Evaluating logistics and transportation capabilities

There are many overlapping responsibilities between the Resources Unit Leader and the Demobilization Unit Leader. In most incidents, there are separate Unit Leaders for these two units. However, in some cases, these two units are managed by a single Leader. If a single

individual is performing both roles, they should be designated as both the Resources Unit Leader and the Demobilization Unit Leader and should separately/distinctly manage each Unit staff.

Technical Specialists

Certain incidents or events may require the use of Technical Specialists who have specialized knowledge and expertise. No specific qualifications are prescribed, as technical specialists usually perform the same duties during an incident as they perform in their everyday jobs, and they are typically certified in their fields or professions. Technical specialists are activated only when needed.

Technical specialists may serve anywhere within the organization depending on factors such as complexity, the span of control, lines of communication, and subject matter expertise. They are often assigned to a 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 are assigned to various jobs temporarily.

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 Specialists Unit is established in the Planning Section to maintain span of control.

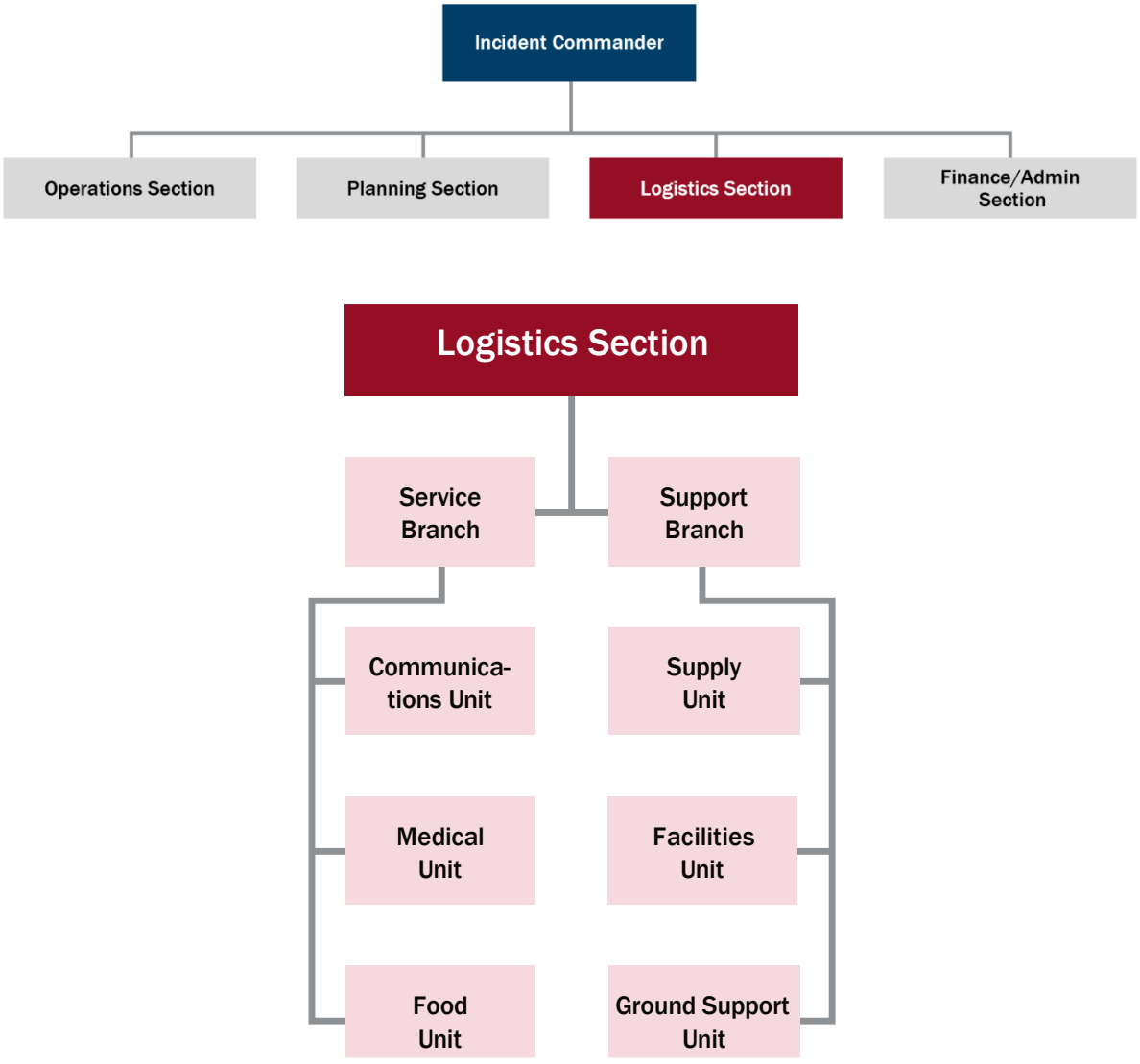
While each incident dictates the need for specific technical expertise, some examples of the more commonly used Technical Specialists include:

- Access and functional needs advisor
- Agricultural specialist
- Behavioral health specialist
- Community representative
- Decontamination specialist
- Environmental impact specialist
- Epidemiologist
- Fire behavior specialist
- Flood control specialist
- Fuels and flammable materials specialist
- Geographic Information Systems Specialist
- Hazardous substance specialist
- Health physicist
- Historical and protected site specialist
- Industrial hygienists
- Intelligence specialist
- Legal advisor
- Meteorologist
- Pharmacist
- Science and technology advisor
- Structural Engineer
- Toxicologist
- Training specialist
- Veterinarian
- Water use specialist

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 can be organized into two branches and six units.

Figure 19: The Logistics Section



Logistics Section Chief

The Logistics Section Chief is responsible for ensuring that incident personnel have the equipment, supplies, transportation, camp facilities, and nutrition they need to meet incident objectives. The Logistics Section supports the entire ICS organization, but its

primary workload is directed at keeping the Operations Section functioning efficiently and effectively by providing resources.

The Logistics Section Chief is responsible for providing for all incident support needs except logistical support for air operations. Logistics is not typically responsible for aviation-specific support. This responsibility belongs to the Air Operations Branch Director or Air Support Group Supervisor within the Operations Branch. Logistics normally provides non-aviation logistical support such as meals, portable toilets, vehicles, and wash stations for aviation operations.

Major responsibilities of the Logistics Section Chief include:

- Providing facilities, transportation, communications, supplies, equipment maintenance and fueling, food and medical services for incident personnel, and resources
- Managing all incident logistics
- Providing logistics input to the Incident Action Plan
- Providing Land Use Agreement information to the Finance/Administration Section's Procurement Unit Leader
- Briefing Logistics Staff as needed
- Identifying anticipated and known incident service and support requirements
- Requesting additional logistics section resources as needed
- Ensuring and overseeing the development of the Communications, Medical, and Traffic Plans as required
- Overseeing demobilization of the Logistics Section and associated resource

Service and Support Branch Directors (SVBD and SUBD)

The Logistics Section may use branches to manage the span of control for the units. However, these branches are only implemented if there is a need to meet the requirements of an incident.

If a Service Branch is implemented, the Service Branch Director's responsibilities include:

- Supervising the operations of the Communications, Medical, and Food Units
- Participating in briefings and planning meetings in the Logistics Section
- Coordinating the activities of Service Branch Units
- Briefing the Logistics Section Chief on Branch activities

If a Support Branch is implemented, the Support Branch Director's responsibilities include:

- Supervising the operations of the Supply, Facilities, and Ground Support Units
- Participating in briefings and planning meetings in the Logistics Section
- Coordinating the activities of Support Branch Units
- Briefing the Logistics Section Chief on Branch activities

Communications Unit Leader

The purpose of the Communications Unit is to plan for and support the effective use of incident communications equipment and facilities.

The Communications Unit is responsible for installing, distributing, testing, tracking, and recovering all communications. This includes both radio and information technology (IT). The Communications Unit obtains and disseminates equipment assignments, frequency assignments, order statuses, adjacent incident information, and equipment availability.

The Communications Unit Leader builds the Incident Radio Communications Plan (ICS Form 205), which is typically set up for radios. They can also build the Communications List (ICS Form 205A) that can be used for cell phones or other communication methods. Personal Identifiable Information must always be protected.

The Communications Unit Leader obtains and disseminates the following information:

- Communications and IT equipment assignments
- Incident frequency assignments
- Status of orders for communications and IT resources
- Adjacent incident communications information
- Communications and IT equipment availability

Supply Unit Leader

The purpose of the Supply Unit is to support responders with the supplies, equipment, and personnel necessary to accomplish incident objectives. Everything that is required for the incident is ordered through the Logistics Section by the Supply Unit Leader. The Supply Unit Leader orders, receives, distributes, and stores supplies and equipment.

Key responsibilities of the Supply Unit Leader include:

- Ordering, receiving, distributing, and storing supplies and equipment that are needed at the incident site to meet incident objectives
- Documenting each resource order from initial request to demobilization
- Recovery and returns of unused supplies

Facilities Unit Leader

The purpose of the Facilities Unit is to provide incident personnel with incident facilities. Facilities can include but are not limited to the Incident Command Post (ICP), incident base, camps, Helibase, Helispot, and staging areas. Facilities also include sleeping and sanitation facilities. Securing facilities can take time.

A key responsibility of the Facilities Unit Leader is to outline incident facilities and determine the requirements for each facility in coordination with Command and General Staff. To

effectively fulfill this function, the Facilities Unit Leader must be able to forecast facilities requirements before they are needed. To accomplish this, the Facilities Unit Leader:

- Identifies facilities requirements
- Prepares layouts of incident facilities
- Notifies all Command and General Staff of the facility layout
- Activates incident facilities

The Facilities Unit Leader provides Land Use Agreement information to the Finance/Administration Section's Procurement Unit Leader.

Ground Support Unit Leader

Ground Support Unit staff provide ground transportation in support of incident operations. They maintain and repair vehicles and mobile ground support equipment and perform inspections on all ground equipment assigned to the incident. The staff oversees supplying fuel for incident mobile equipment and developing and implementing the incident Traffic Plan. Additionally, during major incidents, Ground Support Unit staff maintain a 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.

The Ground Support Unit Leader is responsible for anything related to transportation needs (vehicles, etc.): number, type, how to repair, where to park, separate parking for overhead personnel, ingress and egress, and fueling stations, among other matters.

Key responsibilities of the Ground Support Unit Leader include:

- Developing and implementing the Incident Transportation Plan in coordination with the Operations, Planning, and Logistics Sections
- Planning of traffic flow in camps and bases

Above, we have used the terms Traffic Plan and Transportation Plan in relation to the duties of the Ground Support Unit Leader. A Traffic Plan establishes the flow of traffic in and around an incident base or camp; a Transportation Plan includes the above and also shows traffic in and around the incident area of operations, as well as who is assigned to which vehicle, position assignments, and other factors.

Medical Unit Leader

Medical Unit staff provides 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, assists in controlling the transmission of disease among incident personnel.

The Medical Unit Leader identifies procedures for medical emergencies, declares "major" medical emergencies, and responds to requests for medical aid, medical transportation, and medical supplies. The Medical Unit Leader is responsible for preparing the Medical Plan (ICS Form 206), which indicates:

- Medical procedures for incident personnel involved in medical emergencies
- Incident aid stations
- Hospitals (locations and contact information)
- Transportation (ground and air)
- Steps to follow for a medical emergency
- Communication procedures

The Medical Unit Leader works very closely with the Safety Officer. The Safety Officer is required to approve the Medical Plan (ICS Form 206).

Food Unit Leader

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.

The Food Unit Leader is responsible for meeting the food needs of the entire incident, including all remote locations, as well as providing food for personnel who are unable to leave tactical field assignments. The Food Unit Leader is responsible for ensuring that all incident personnel are adequately fed and hydrated. This responsibility also entails determining the best method for delivering sanitary food and water. Both adequate forecast and delivery of food, water, and appropriate cooking and quality of food are key concerns of the Food Unit Leader.

The Food Unit Leader determines and fulfills meal requirements at the incident. This means that the Food Unit Leader is responsible for ensuring the following food-related supplies and equipment activities:

- Ordering
- Relocating
- Reducing
- Releasing
- Reassigning
- Canceling

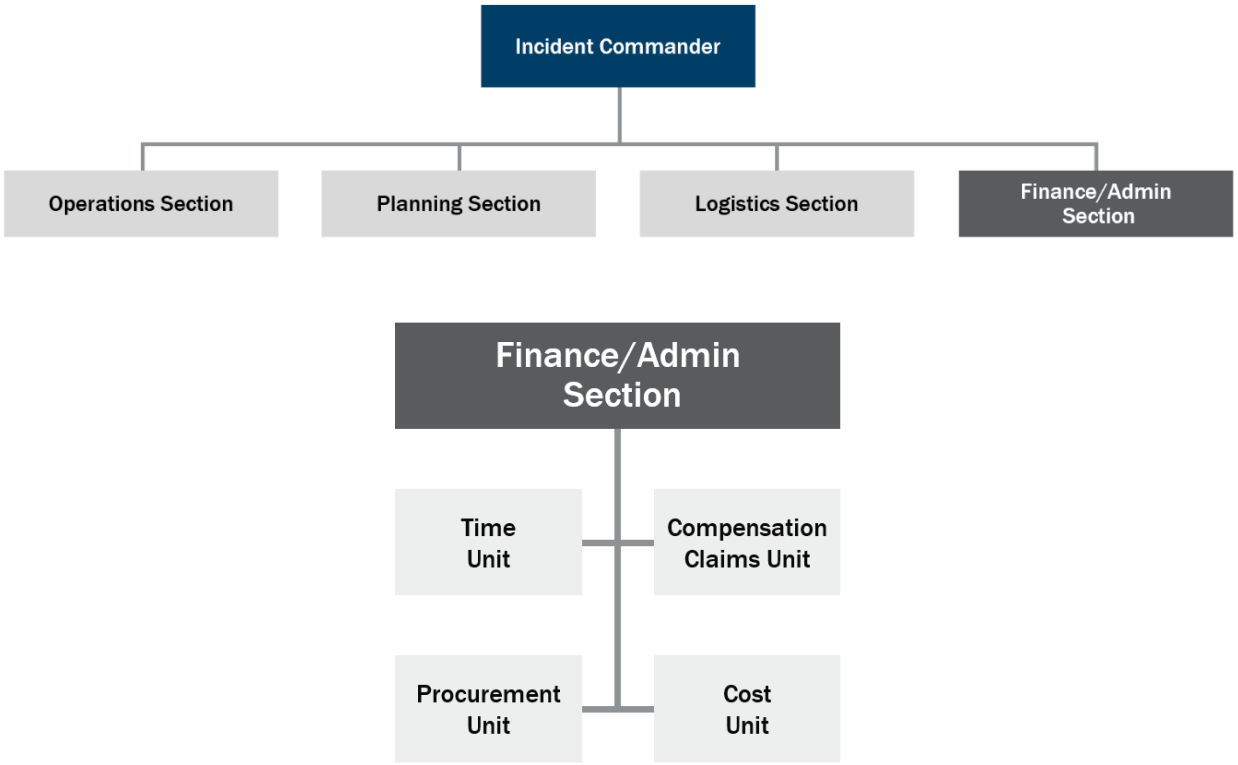
Finance/Administration Section

The Finance/Administration Section is responsible for managing all financial aspects of an incident. Ideally, the Finance/Administration Section Chief will be familiar with accounting procedures and spending authority rules established by the lead fiscal agency for the

incident. The Incident Commander or Unified Command establishes a Finance/Administration Section when financial and/or administrative services are needed to support incident management activities.

Large or evolving scenarios involve significant funding from multiple sources. An on-site Finance/Administration Section may not be required in every incident. The Section will be activated only when the involved agencies have a specific need for financial services. If a Finance/Administration Section is not established, the Finance and Administrative functions will still have to be performed for the incident. This may be accomplished off-site by finance/administration staff of the jurisdiction assigned to support the incident in collaboration with other finance/administrative staff from responding agencies.

Figure 20: The Finance/Administration Section



Finance/Administration Section Chief

The Finance/Administration Section Chief monitors multiple funding sources and tracks and reports accrued costs to the Incident Commander or Unified Command. This allows 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.

The Finance/Administration Section Chief oversees expenditures to ensure that they are in accordance with applicable laws, policies, and procedures. Close coordination with the

Planning and Logistics Sections is essential so that operational records can be regulated with financial documents.

Major responsibilities of the Finance/Administration Section Chief are to:

- Manage all financial aspects of an incident
- Provide financial and cost analysis information as requested
- Ensure compensation and claims functions are being addressed relative to the incident
- Gather pertinent information from briefings with responsible agencies
- Develop an operating plan for the Finance/Administration Section and fill Section supply and support needs
- Meet with assisting and cooperating agency representatives as needed
- Maintain daily contact with agency(s) headquarters on finance matters
- Ensure that personnel time records are completed accurately and transmitted to home agencies, if needed
- Ensure that all obligation documents initiated at the incident are properly prepared and completed
- Brief agency administrative personnel on all incident-related financial issues needing attention or follow-up
- Provide input to the IAP
- Coordinate procurement, contracting, and financial agreements, (e.g., land use, cost apportionment, etc.) as needed

Time Unit Leader

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 is responsible for collecting, recording, and maintaining all-time data and cumulative time records. The timekeeping function is different from a payroll function. Timekeeping is to ensure that all hours worked are accurately documented.

Procurement Unit Leader

The Procurement Unit staff manages all financial matters pertaining to leases and vendor contracts.

The Procurement Unit Leader is responsible for administering vendor contracts, leases, and fiscal agreements. Responsibilities may vary depending on contracting authorities and regulations.

Compensation/Claims Unit Leader

Compensation and Claims Unit staff are responsible for financial concerns resulting from property damage, injuries, or fatalities at the incident.

The Compensation/Claims Unit Leader is responsible for the overall management of compensation for injury and claims-related activities. The Compensation/Claims Unit is not responsible for accidents or damages amongst the public; they are only responsible for the incident responders' compensation and claims support needs.

Cost Unit Leader

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.

The Cost Unit Leader is responsible for collecting all cost data, performing cost-effectiveness analyses, and providing cost estimates and cost-saving recommendations for the incident. The Cost Unit Leader ensures that cost estimates for resource utilization are provided to the Planning Section.

Intelligence/Investigations Function (I/I)

Many domestic incidents, such as natural disasters or industrial accidents, have an obvious cause and origin. However, other domestic incidents, such as large-scale fires, public health emergencies, explosions, transportation incidents (e.g., train derailments, airplane crashes, bridge collapses), active shooters, terrorist attacks, or other incidents that cause mass injuries or fatalities, require an intelligence or investigative component to determine the cause and origin of the incident and/or support incident/disaster operations.

The Intelligence/Investigations function within ICS provides a flexible framework that allows for the integration of intelligence/investigations. Intelligence/Investigations supports the sharing of information across all levels of government, disciplines, and security domains. Situational awareness is enhanced by the Intelligence/Investigations function through the sharing of pre- and post-incident information, intelligence, and real-time incident intelligence and investigation activities.

The scalability and flexibility of NIMS allows the Intelligence/Investigations function to be seamlessly integrated with the other functions of ICS. The Intelligence/Investigations function provides a framework that allows for the integration of intelligence and information collection, analysis, and sharing, as well as investigations that identify the cause and origin of an incident. If the incident is determined to be a criminal event, the Intelligence/Investigations function leads to the identification, apprehension, and prosecution of the perpetrator. The Intelligence/Investigations function can be used for planned events as well as incidents.

The mission of the Intelligence/Investigations function is to ensure that all intelligence/investigations operations and activities are properly managed, coordinated, and directed to:

- Prevent/Deter potential unlawful activity, incidents, and/or attacks
- Collect, process, analyze, secure, and disseminate information and intelligence
- Identify, document, process, collect probative evidence, and create a chain of custody for safeguarding, examining, analyzing, and storing the evidence
- Conduct investigations to identify, apprehend, and prosecute perpetrators
- Serve as a conduit to provide situational awareness (local and national)
- Inform and support life safety, including the safety and security of all response personnel

Intelligence/Investigations Section Chief, Branch Director, or Group Supervisor

The title of the Intelligence/Investigations function lead will vary based on the placement of Intelligence/Investigations within the incident command organization.

- As a General Staff section, they would be called the Intelligence/Investigations Section Chief.
- As a Branch under Operations or Planning, they would be called the Intelligence/Investigations Unit Leader.
- As a Group under Operations, they would be called the Intelligence/Investigations Group Supervisor.

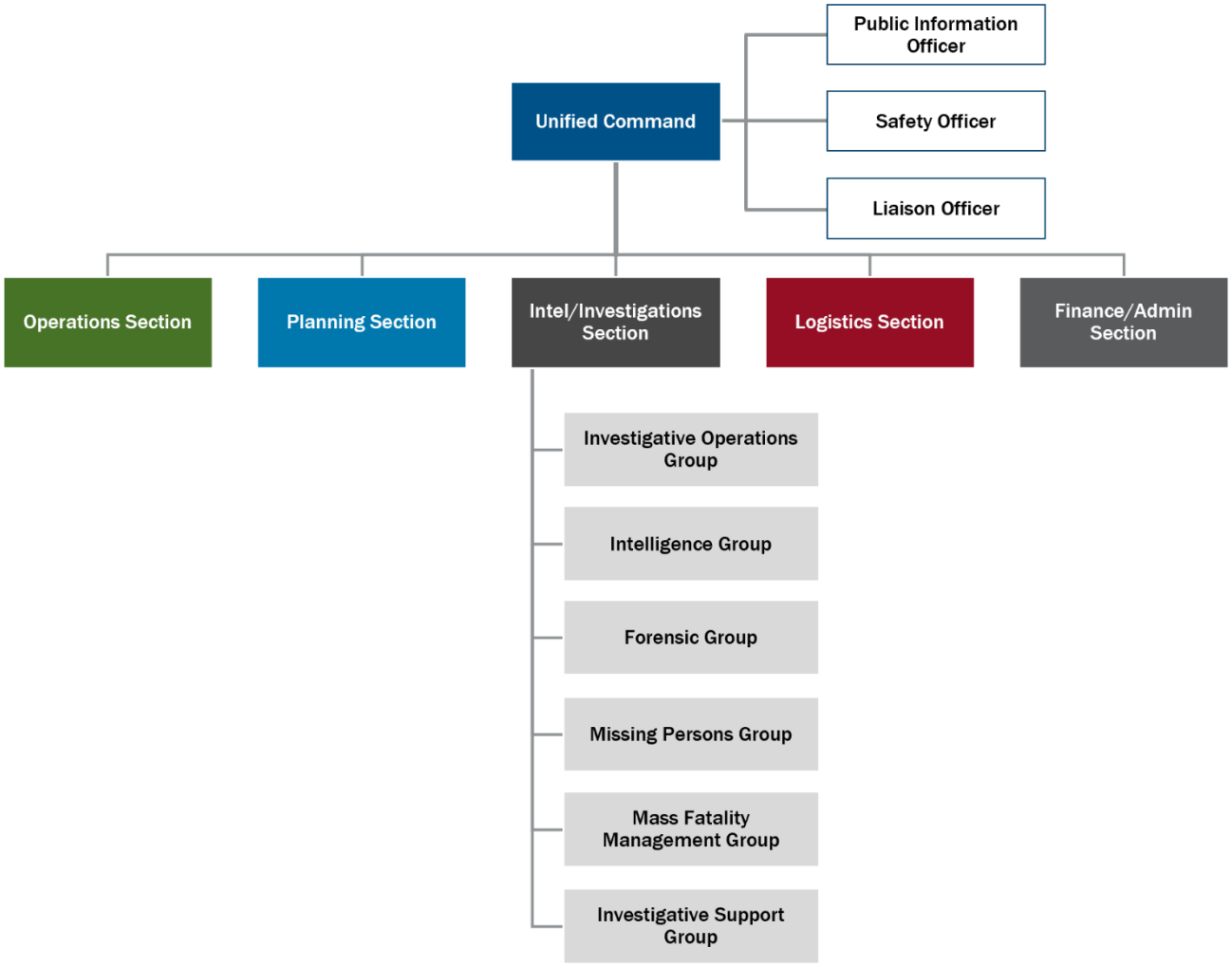
Regardless of the Intelligence/Investigation placement within the ICS staff, the Intelligence/Investigations lead is responsible for overseeing investigative and intelligence-gathering efforts for the incident. In some instances, the work of the Intelligence/Investigations Section may require the Intelligence/Investigations to be organized as a separate section. In these situations, the Intelligence/Investigation lead may activate one or more Groups within the Intelligence/Investigations Section and designate a Group Supervisor for each to address the span of control issues. When an investigation requires an extremely large number of personnel, Intelligence/Investigations may also utilize Branches to address span of control issues. The NIMS Intelligence/Investigations Function Guidance and Field Operations Guide (October 2013) outlines six Groups that may be activated as needed under an Intelligence/Investigations Section:

- Investigative Operations Group – manages the overall investigative effort.
- Intelligence Group – manages information intake and assessment, operations security, operational security, information security, and information/intelligence management.
- Forensic Group – manages the crime scenes and directs the processing of the forensic evidence, digital and multimedia evidence, and decedents.

- Missing Persons Group - directs missing persons operations and activities, as well as Family Assistance Center activities involving missing persons.
- Mass Fatality Management Group – directs intelligence/investigations activities involving mass fatality management operations, including Family Assistance Center activities involving decedents and unidentified persons.
- Investigative Support Group – provides specialized resources for Intelligence/Investigations by working closely with the Command and General Staff, particularly the Logistics Section and Planning Section, to ensure that the Intelligence/Investigations Section has the necessary resources, services, and support it requires. The role of the Intelligence/Investigations lead is not only to oversee investigation and intelligence activities but also all aspects of incident management related to the Intelligence/Investigations Section. This may include intelligence and investigation, human services, demobilization, communications, and other activities.

For access to the NIMS Intelligence/Investigations Function Guidance and Field Operations Guide, visit: https://www.fema.gov/sites/default/files/2020-07/fema_nims_intelligence-investigations-function-guidance-oct-2013.pdf

Figure 21: The Intelligence/Investigations Organized as a Separate Section with Groups



Chapter 3: Supervision and Management

Defining Supervision

Supervision is overseeing the productivity and performance of people. It is task-oriented; tasking personnel with specific assignments, providing instruction on how to perform specific tasks, monitoring personnel performance of tasks, and holding personnel accountable for task performance quality and results.

Defining Management

Management is the coordination of people and resources to achieve desired outcomes. This entails identifying objectives and goals, developing a plan to achieve them, identifying personnel and resource requirements, directing the efforts of personnel, monitoring how effectively personnel implements the plan, assessing whether the objectives are achieved, and changing strategies and tactics, as needed, to ensure objectives are achieved.

The Management Cycle

The management cycle is a process that organizational leaders follow to ensure that personnel work effectively to achieve objectives. There are many management cycle models. Most reflect the following steps: plan, organize, staff, direct, control, and evaluate.

Note: The management cycle presented is a model for understanding higher-level management processes. This should not be confused with the ICS Operational Period Planning Cycle (the Planning P).

Management Cycle Activities

Plan	Determine what needs to happen in the future and create a plan of action.
Organize	Define the structure that will be used by the organizational resources to carry out the plan.
Staff	Analyzing job tasks that support plan accomplishment and putting in place personnel with the necessary knowledge, skills, and abilities to perform those tasks effectively and efficiently.
Direct	Assign tasks and direct, guide, and motivate personnel to achieve the objective.
Control	Assess actual progress towards planned outcomes, and adjust, as necessary, to ensure that the desired outcomes are achieved (sometimes referred to as monitoring and evaluating).

Defining Leadership

Leadership has been defined in many different ways. At its core, leadership is a process of social influence, which maximizes the efforts of others toward the achievement of a defined outcome. A leader establishes the direction to achieve the desired outcome and then influences people to follow that direction and achieve that desired outcome. By this definition, anybody within the organization can demonstrate leadership, even if they are not formally assigned management or supervisory positions.

The following quotes define leadership:

> *"Effective leadership is putting first things first. Effective management is discipline, carrying it out." --Stephen Covey*
>
> *"The greatest leader is not necessarily the one who does the greatest things. He is the one that gets the people to do the greatest things." --Ronald Reagan*
>
> *"It is better to lead from behind and to put others in front, especially when you celebrate victory when nice things occur. You take the front line when there is danger. Then people will appreciate your leadership." --Nelson Mandela*

Leadership Traits and Principles

Leadership is a skill that requires training and development regardless of any natural leadership ability you may possess. Though leadership may seem more natural for some, most individuals can improve their leadership skills with education and practice.

Leadership principles are the ideals that guide decisions and actions. They are the internal standards one refers to when one struggles with a tough decision or experiences moments of doubt. Shown here is a list of some of the traits, and principles of successful leaders:

Leadership Traits	Leadership Principles
Vision	Know and be true to yourself
Commitment/Dedication	Look out for your people
Integrity	Lead by example
Empathy	Seek innovative solutions
Honesty	Inspire others
Authenticity	Admit mistakes
Patience	Always seek to learn
Courage	Take ownership
Transparency	Earn trust
Humility	
Resilience	
Adaptability	
Accountability	
Passion	
Excellence	

Leadership and Interpersonal Skills

Problem-Solving and Decision-Making

Problem-solving and decision-making are two closely related leadership activities. Problem-solving is a set of activities designed to analyze a situation systematically and generate, implement, and evaluate solutions. Decision-making is making choices at each step of the problem-solving process.

Analytical Approach

It is helpful to have a defined process to follow to solve a problem or make a decision. The process need not be complex—in fact, in many cases, simpler is better. There are many different decision-making models to choose from; a commonly used five-step process is presented in this table.

Step 1: Identify the Problem	Define the perceived existing or anticipated problem.

Step 2: Explore Alternatives	Generate alternative approaches to the problem and evaluate them.
Step 3: Select an Alternative	Select the alternative most likely to solve the problem (achievable, greatest advantages, least unacceptable disadvantages).
Step 4: Implement the Solution	Determine objectives or measurable targets. Develop an action plan (what steps are needed). Identify needed resources. Identify details (who, what, when, where, how).
Step 5: Evaluate the Situation (ongoing process)	Monitor progress and evaluate the approach and progress of the plan toward the desired outcome (discern changes in the situation, evaluate changes in resource requirement, determine if an alternative approach is required).

Quality of Information

Data used in decision-making must be accurate and reliable. The old adage, "Garbage In = Garbage Out" (GIGO), is especially true in decision-making. Faulty or inadequate information results in poor decisions—sometimes with profound consequences. Thoroughly screen the information used in making decisions!

Communication

Communication involves establishing a personal connection with the audience, reaching out to them with your message. To communicate effectively—whether your audience is a single individual or a large group—it is helpful to understand the basic skills that form the building blocks of effective communication.

Formal Communications

Formal communication follows the chain of command and, as the incident organization grows to meet the needs of the incident, care must be taken to ensure that information transfer is handled effectively. Formal communication requires that orders, directives, resource requests, and status changes must follow the hierarchy of command unless otherwise directed.

Informal Communications

Informal communication is used when exchanging incident or event information. It is not used for formal requests for additional resources or tasking working assignments. A significant amount of interaction and informal communications occur outside of the meeting/briefings. This is necessary for Situational Awareness (SA), Common Operating

Picture (COP), coordination, updates, etc., between sections and Command and General Staff. We need to encourage constant communication within the team.

Oral Communication

Oral communication is a fluid and dynamic process shaped by both the speaker and the audience. While you are communicating and someone else is listening, you are also receiving verbal and non-verbal clues from the listener. When you are listening to someone else, you are also receiving both verbal and non-verbal input. Listening is critical for successful communication and almost half of our communication time is spent listening.

Barriers to Effective Listening

Barriers to effective listening can be external or internal. External roadblocks can include distracters such as noise, an uncomfortable temperature or seating, or an inappropriate location. So, try to be aware of external roadblocks and offset them if possible.

Internal roadblocks to effective listening include conditions or reactions within the speaker or audience, such as emotional interference or defensiveness, hearing only facts and not perceiving feelings, hearing what is expected instead of what is said, and resisting change.

When listening, try to keep an open mind, maintain eye contact and show interest, listen for the central themes, and consider the speaker's nonverbal behaviors and tone of voice.

While listening, avoid being judgmental, interrupting the speaker, formulating a response as they are talking, and allowing the message to become distorted based on your preconceived ideas.

Active Listening

Active listening involves listening with empathy and paraphrasing. Empathy refers to seeking to understand the feelings of others. When you listen with empathy, you don't just hear words, you try to understand thoughts, beliefs, and feelings. Empathic listening is highly effective and takes practice.

Paraphrasing is an effective active listening technique. When you paraphrase, you ensure clear understanding by restating the speaker's main points in your own words. Paraphrasing also provides important feedback that helps speakers gauge how well they are getting their message across.

Nonverbal Cues

Nonverbal gestures speak volumes. Body language alone, including facial expressions, gestures, eye contact, and tone of voice, accounts for more than 90 percent of the message we send to others. Our words account for only seven percent of the message.

If you understand nonverbal cues, you can use them to reinforce your message. You can also use nonverbal understanding to read your audience and gather real-time feedback about whether you are communicating successfully.

It is important to align nonverbal clues with your message. When nonverbal cues do not match the spoken words, it can result in confusion and mixed messages. When nonverbal cues contradict or supersede verbal messages, listeners instinctively react with caution or even mistrust.

Using Your Voice Effectively

Public speaking does not come naturally to everyone, but it is a skill that can be learned. Understanding the basics and practicing will make most of us better speakers. It is also helpful to begin small (e.g., a small group and informal setting) and work up to greater challenges.

When presenting to an audience, be sure to use clear and concise language, speak loud enough to be heard, and change the pace of your presentation. To make yourself heard, imagine that you are talking directly to the person who is farthest away, not the person in the front row. If the room is large or there is a lot of background noise, use a microphone if it is available.

Written Communication

Depending on your role in the ICS organization, your requirement to perform written communications tasks may vary greatly. Most ICS leaders have some requirements to create clear, concise written products. You must be able to communicate in writing to reach a broad audience that includes response partners and other colleagues, private sector and nonprofit organizations, the media, and diverse public. This is particularly true for positions such as the Public Information Officer, who is responsible for messaging multiple stakeholders.

Communicating with the Public

Communicating effectively with your community means communicating with the whole community. Communities are diverse. They include people of all ages and varied cultural backgrounds, individuals with disabilities, and people with other access and functional needs. To ensure that your public messages are clearly understood, use plain language, avoid acronyms and jargon, and keep sentence structure simple. It is a best practice to compose messages that can be understood at an 8th-grade (or lower) reading level and to make messages available in the languages spoken within the affected communities.

Collaboration

Collaboration is the process by which people work together as a team toward a common goal. To be successful, the team members must collaborate.

Collaboration necessitates the flexibility to reach an agreement on shared goals and priorities and humility to learn from others' ways of doing things. It requires the commitment to participate in shared decision-making, willingness to share information, resources, and tasks, and professional respect for individual team members.

Collaboration does not come automatically. Challenges to collaboration can come from differences between agencies and organizations, such as terminology, experiences, mission, and culture. Building a team that works well together takes time and effort and typically evolves through the following stages:

1. Forming: Individuals come together as a team. During this stage, the team members may be unfamiliar with each other and uncertain of their roles on the team.
2. Storming: Team members become impatient, disillusioned, and may disagree.
3. Norming: Team members accept their roles and focus on the process.
4. Performing: Team members work well together and make progress toward the goal.
5. Adjourning: After their task is accomplished, team members may feel pride in their achievement and some sadness that the experience is ending.

Facilitation

As a leader, you will often have to ensure that meetings take place on time and remain organized. Meetings present complex challenges with various components that need a significant amount of time and attention away from your other duties. If not effectively managed, meetings can divert your attention from other position responsibilities. Meetings should always be held for a defined purpose, for a defined period. Your facilitation of meetings should focus on achieving that purpose completely and in the minimum time necessary.

Time Management

Time management is critical during an incident. Leaders need to understand their priorities and desired outcomes and have a plan for how they will manage their time to achieve these outcomes. Leaders must constantly evaluate how they are using their time against their defined priorities. They must stay on track. High-priority duties, responsibilities, and tasks may not be completed if too much time is diverted to lower-priority activities.

Plans, schedules, and checklists are tools to help a leader manage their time. Meeting agendas and briefings that define meeting purpose and timeline can keep meetings on topic and schedule.

Political Savvy

Political savvy is a positive attribute. Many people have negative feelings about being "political," but "political savvy" is fundamentally the ability to understand the people you are interacting with in the incident. Incident personnel must be cognizant of local political dynamics to be successful in their mission. Failure to recognize such elements can easily result in frustration and not meeting the needs of locals in their mission. A clear understanding of these considerations and the ability to navigate them are important.

Flexibility

Flexibility is a NIMS Guiding Principle. All leaders must be flexible when undertaking a role in disaster response and recovery. Because numerous factors may change during an incident response, flexibility and a willingness to be adaptable and creative in strategies and tactics are often necessary to manage incidents with varying hazards, geography, demographics, climate, and cultural and organizational authorities.

Goal Orientation

The NIMS Management Characteristic "Management by Objectives" is goal oriented. It is the management of operations to achieve specific objectives. Goal orientation ensures a shared focus for all ICS functions. This common focus should be shared across the ICS organization. Field resources must "see the big picture" and understand why actions are required.

Conflict Resolution

Conflict occurs when two or more parties have dissimilar needs, desires, ideas, or goals and the interests of one party impinges on the interests of another. Although conflict is sometimes uncomfortable, it is important to understand that it is a natural part of human interaction. Conflict can be more prevalent in the chaos surrounding incident response. If managed effectively, a conflict that is effectively resolved can contribute to mission accomplishment.

Healthy conflict requires focusing on the "what" rather than the "who." That is, what accomplishes the mission or serves the common good rather than who is involved. Trust enables a team to engage in healthy conflict and build cohesion rather than devolving into a conflict that divides. Team members will be more willing to engage in constructive debate and provide insight and judgment when they know others on the team listen to them and take their suggestions and arguments seriously. A foundation of trust encourages team members to contribute their insights and judgments when appropriate.

Coaching and Evaluation

Coaching is helping trainees build knowledge, skills, and abilities to perform in a specific position. The National Incident Management System (NIMS) Guideline for the National

Qualification System (NQS) defines a coach as an individual with specific job skills and expertise which gives instructions and mentoring to guide a trainee in learning applicable practices, methods, and skills that can lead to PTB task completions. (NIMS NQS, 2019)

Evaluation is the act of verifying that the trainee knows how to do a certain task. The NIMS Guideline for the NQS defines an evaluator as an individual authorized by an Authority Having Jurisdiction to observe, document, and complete evaluation records on a trainee based on a Position Task Book. Coaches and evaluators work together to guide trainees through the qualification process.

For tips on becoming a great mentor, go to: https://www.usfa.fema.gov/blog/cb-042319.html.

Responsibilities of All ICS Leaders

In the remainder of this chapter, we will review the following responsibilities shared by all ICS leaders:

- Communicate Leaders Intent
- Assign and Track Tasks
- Participate in Meetings and Briefings
- Promote Situational Awareness and Common Operating Picture
- Manage Information and Documentation
- Promote Safety and Security
- Lead Assigned Staff
- Manage Assigned Resources

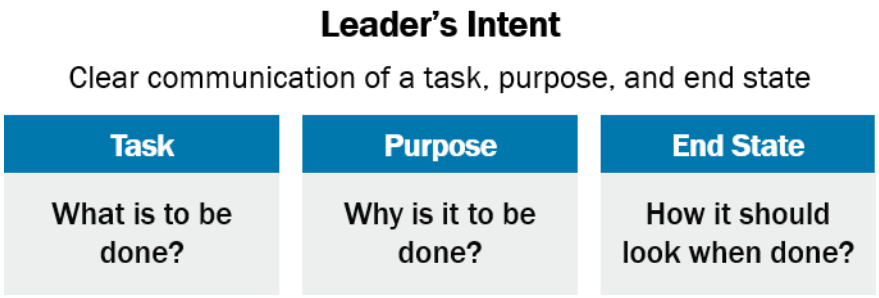
Communicate Leader's Intent

Leader's intent is an over-arching statement related to a desired end-state for the incident. Leader's intent frames the parameters of success. It defines what needs to be accomplished. It is not intended to formally establish operational directives and is not tactical in nature.

Leader's intent is a clear, concise statement about what people must do to succeed in their assignments. It delineates three essential components:

1. Task. What is the objective or goal of the assignment?
2. Purpose. Why the assignment needs to be done.
3. End state. How the situation should look when the assignment is successfully completed.

Figure 22: Leader's Intent



Communicating Leader's intent

In fast-moving, dynamic situations, top-level decision-makers cannot always incorporate the latest information into a formal planning process and redirect people to action within a reasonable timeframe. When rapidly evolving, chaotic conditions interfere with the ability of the Incident Command to issue new directions in real-time, a leader's intent can help those closest to the incident to respond to the conditions on the ground based on an understanding of overall direction and priorities. It allows them to adapt plans and exercise initiative to accomplish the objective when unanticipated opportunities arise or when the original plan can no longer achieve the desired outcome.

Defining the desired end state helps leaders in the development of incident objectives, priorities, strategies, Management Action Points, and contingency plans.

The following statements provide examples of what Leader's Intent may look like during an incident:

"We do not have good situational awareness on how the storm affected our community. We need to focus our efforts on rapid completion of a full damage assessment for our community so that we can submit our disaster summary outline to the state in three days."

"On the other side of this creek is a large lumber production area that is a major part of the economy of this community. Our overall operational approach must protect that area from the fire to mitigate long-term economic damage to the community."

Assign and Track Tasks

A leader normally cannot perform or even directly supervise everything occurring under them. An effective leader delegates broad responsibilities to team members, allows team managers to manage the details of preparation and execution, and holds them accountable for their results.

Delegating responsibilities to capable personnel has many advantages. It distributes the workload, which results in higher efficiency, increased motivation, and develops the skills of

the workforce. It allows the leader to focus on issuing guidance, tracking progress, and making necessary course corrections. Finally, delegation provides opportunities for subordinates to develop their own leadership skills.

While supervisors must delegate tasks, working together as a team can help ensure that the deadlines are met. Each member of the ICS organization must recognize the tasks they are to accomplish and what interactions will be necessary to complete the job.

When assigning and delegating tasks to staff, it is important to focus on *what* needs to be done and not *how* it should be done. Tasks should be stated in a manner that is both clear but also allows flexibility.

Some ways to achieve this include:

- **Prioritize Assignments.** Supervisors must prioritize assignments within the team. Many times, there are more tasks to be done than staff to do them. Understanding the relative priority of objectives, strategies, tactics, and tasks is important. Everything you have to accomplish is likely a priority, but which things are of the greatest importance and which are lesser. When setting priorities, consider the incident priorities defined in the National Response Framework. These priorities are save lives, protect property and the environment, stabilize the incident, meet human needs by stabilizing Community Lifelines, and prepare for Recovery. Use of this priorities framework can help to focus efforts to navigate multiple priorities in an organized and logical manner during incident response. Another helpful way to understand priorities is to pay attention to your supervisor's intentions. After an incident, initial assessments of the community lifelines (i.e., whether they are impacted and to what extent) help establish incident priorities and objectives that drive response actions. Continuously reassessing the status of community lifelines enables decision-makers to adjust operations in ways that can accelerate incident stabilization.
- **Assign/Delegate Completion of Tasks to Staff.** Delegation of tasks is vital to utilizing a team effort to achieve objectives. When delegating, you should provide clear direction and expectations. You should assign personnel according to their ICS qualifications, experience, skills, and ability. Identify the appropriate person for the task.
- **Establish Performance Requirements.** During an incident, it is important that the subordinates clearly understand what is expected of them. Workers need to know what is expected to achieve outcomes. Prepare the person by clearly stating desired outcomes while encouraging innovation. Ensure they understand the identified priorities, expectations, established timeframes and schedules, and the need to work as a team.
- **Empower Personnel.** Due to the nature of the ICS organization's responsibilities, it must constantly lean forward and always be prepared to take decisive action. Members of the ICS organization must be empowered to take actions expeditiously to achieve desired outcomes. To fulfill its mission and live up to its core values, a professional workforce of

motivated employees who are empowered and equipped to act is critical. Empowerment is achieved when those closest to the need are ready and able to act and make informed, prompt decisions based on the appropriate authorities, principles, and practices. Ensure that each subordinate has the necessary authority to accomplish their assigned job properly.

- **Track.** Tracking of tasking is keeping a record of the tasks that you have assigned and the status of each assignment. This is a shared responsibility of both the team and the supervisor. Your subordinates should understand the task status and overall goals of the entire team. A tracking mechanism should be set up to ensure that staff is clear on assignments. Many teams utilize a spreadsheet or similar document to track this.
- **Monitor.** When delegating tasks, supervisors must remember that they still have an obligation to monitor the delegated work to ensure that they are receiving the support they need and to verify that delegated tasks are being accomplished. Supervisors must monitor how the staff is progressing in any assigned task. Supervisors can effectively enable staff to self-direct their efforts to complete assignments by setting guidelines, deadlines, and deliverables. Routine meetings within the team and units will also assist in determining progress and impediments to success.
- **Assess Progress.** Gain situational awareness by "walking around" is one of the key points of being an effective supervisor. Having the ability to observe operations and be seen by your organization establishes not only command presence, but also shows engagement in the incident response. Supervisors should maintain enough contact to monitor progress and provide support without "hovering" or micromanaging. "Walking around" can provide opportunities for you to coach and mentor your subordinates as they are performing their assigned duties, responsibilities, and tasks.
- **Hold Staff Accountable.** Staff should be held accountable for their actions and for meeting agreed-upon outcomes based on documented issues. The use of written objectives and tasking is vital in holding staff to a standard. When giving task performance feedback, it should not only focus on deficiencies, but you should also acknowledge success and give credit where it is due.
- **Solicit Feedback.** Interact with staff regularly. Encourage participation and communications and remain open to suggestions, feedback, and dissenting opinions. Actively seek and allow time to receive feedback from your subordinates. At the same time, be aware of the potential for "group think."
- **Adjust Work Assignments.** Make sure that you are monitoring the activity of your subordinates. Over time, the workload will change. Some tasks may be completed, new tasks will emerge, and some tasks may require increased or decreased efforts. You may have to shift assignments around to help the people who are most overwhelmed accomplish their assignments.

Participate in Meetings and Briefings

The purpose of meetings and briefings held during each operational period in the incident action planning cycle is to ensure that information is shared and that decisions are made with the input of those stakeholders who play a direct role or support an operation. In an ICS organization, the Planning Section Chief is responsible for facilitating most meetings and briefings. Participants must stick to the meeting agenda and remain focused on the task at hand. The agenda assists those expected to speak or present are recognized in a logical order. Speakers should focus on their responsibilities and make sure that they are ready with the information that they are to discuss or present.

Incident Action Planning Meetings and Briefings

The Planning Cycle requires the completion of five major meetings and briefings in each operational period. These will be discussed in greater detail in Chapter 5, Incident Planning.

- Strategy Meeting/Command and General Staff Meeting
- Tactics Meeting
- Planning Meeting
- Incident Action Plan Preparation and Approval
- Operational Period Briefing

Section Briefings

Section chiefs also may call meetings of their staff at any time. This is a time for the section chief to assess progress, address concerns, or disseminate information to the section personnel.

Unit Briefings

Much like section briefings, these meetings are intended to address matters that are related to a single ICS unit, such as the Resources Unit, Facilities Unit, or Procurement Unit.

ICS Organizational Briefings and Debriefing

The ICS organization may hold a briefing on crucial information changes at any time during an incident.

A debriefing of the team's performance at the incident may occur during or at the end of a mission. This is a meeting for team members only. It is a time to discuss lessons learned, performance issues, changes in team practices, etc. It should be an open and frank discussion among members, sections, units, etc. This debriefing intends to improve team performance in the future.

Other Important ICS Organization Meetings

- Command and General Staff Meetings (for some ICS organizations such as All-Hazards IMTs, this is a separate meeting from the NIMS Strategy/Command and General Staff Meeting)
- Transition Meetings
- Cooperation meetings
- Debrief or Closeout Meeting
- Public Meetings
- Demobilization Meetings
- Agency-Specific Reviews or After-Action Meetings

Promote Situational Awareness and Common Operating Picture

Situational Awareness and Common Operating Picture help decision-makers generate timely, well-informed, and well-coordinated decisions to ensure the safety of personnel, the efficiency of operations, and the accomplishment of objectives.

Communication and information sharing are essential to incident size-up, evaluation, maintaining Situational Awareness, and a Common Operating Picture. Incident information shapes the operational strategies, tactics, safety considerations, etc.

Maintain Situational Awareness

Situational awareness is a combination of pre-existing knowledge with information gathered from the current situation. Situational awareness concerns building a clear perception of one's current circumstances based on accurate and timely new information.

The U.S. Coast Guard defines Situational Awareness as "the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission." More simply, you must know what is going on around you.

Situational awareness, like safety, is the responsibility of everyone. Without a clear perception of the current situation, any efforts to manage risk, maintain personal safety, and look out for the safety of others may be severely compromised or misguided.

In an ICS organization, the Situation Unit provides a focused effort for situational awareness. However, all ICS leaders have a responsibility to contribute to situational awareness. Maintaining situational awareness requires being continuously in touch with team members and co-workers. It requires monitoring how team members are performing, coordinating activities, and being available if team members or co-workers need to communicate. Following a "see and be seen" strategy is an effective way to ensure active engagement.

Situational awareness commonly includes elements such as:

- What is it?
- What happened?
- Where have we been?
- Where are we now?

- Where are we going?
- What is going to happen next?
- What can we do next?
- What progress has been made?
- What is the incident extent?
- What is the incident growth potential?
- What are the threats?
- What are the opportunities?

Participation in Incident Action Planning Meetings and briefings (as required) is one of the most important tools for gathering and disseminating information during an incident. It is also important to provide regular updates to your supervisor on your Section, Branch, Division/Group, Unit, or Strike Team/Task Force Status to ensure that they are aware of your status and any issues that may be hindering their success.

Maintain a Common Operating Picture

Common Operating Picture is a continuously updated overview of incident information that all incident personnel shares. It ensures that all parts of the incident response operate from a common baseline of information. It allows decision-makers to operate based on a shared set of validated information. Common Operating Picture helps decision-makers generate timely and well-informed decisions to ensure the safety of personnel and the accomplishment of objectives. All ICS leaders must share situational awareness to develop a Common Operating Picture. (DHS COP, 2012)

Frequency of Communications

Most of the information flow within the ICS organization will occur during the meetings and briefings conducted via the Planning P process. This does not preclude other formal communication within the chain of command or informal communication between different ICS functions and team members.

Brief Superiors

Accomplishments and problems should be discussed with your immediate supervisor in the ICS chain of command. Pertinent situational awareness information should also be brought forward in the Operational Period Planning Cycle meetings, during the Command and General Staff Meeting, and during other meetings of the staff.

Critical Reporting Thresholds

The Incident Commander or Unified Command will usually identify “critical reporting thresholds.” These are also sometimes referred to as “Critical Information Requirements.” This is the information that must be reported to them immediately. In most cases, this information is forwarded to the Agency Administrator and/or Emergency Operations Center for the jurisdiction. (USFA, 2014) Some examples of critical reporting thresholds include:

- Serious injury (requiring transportation to a medical facility) or fatality to a responder

- Substantial escalation in the size or complexity of the incident
- Rapidly emerging issues that significantly increase the evaluated risk to life safety
- Significant change in strategy during the current operational period
- Event that draws significant political, media, or social interest
- Management Action Point identified by the Incident Commander or Unified Command

Addressing Critical Issues

Critical issues affecting the success of the team should be discussed in Command and General Staff meetings unless exigent safety circumstances demand immediate attention. The chain of command should be followed unless an immediate threat to life is present.

Report Unexpected Occurrences

All staff should promptly report any unexpected occurrences, including injuries, damages, illness, or exposures, to their supervisor. Command and general staff should review such matters to determine the causes and any mitigations needed to ensure that the incidents are not repeated. All occurrences should be well documented not only for current operations but in case there are any delayed or long-term issues related to the occurrence.

Unexpected occurrences are adverse events not consistent with the desired operation of the incident. It causes an unexpected outcome and/or an unexpected need for intervention. A "near miss" is something that has the potential for causing injury, illness, or death but was prevented by a fortunate break in the chain of events.

Serious unexpected occurrences must immediately be reported to the proper chain of command while simultaneously providing medical care for the injured, preserving evidence, factually documenting the occurrence, and maintaining confidentiality. Reporting a near-miss event through the chain of command should be encouraged and non-punitive. This promotes an environment where learning from the impact of the error can prevent and reduce responder injuries and fatalities.

Manage Information and Documentation

Ensure Thorough and Accurate Documentation

Supervisors are responsible for ensuring that staff actions and documentation are accurate and complete. This includes all documents, such as personnel evaluations, equipment time records, personnel time records, accident reports, and mechanical inspections. Ensure that all staff complete their timesheets and that they are accurate and complete. Documentation from the Activity Log (ICS Form 214) should match timesheets.

Leaders should use the Activity Log (ICS Form 214) or a similar tool to document their activities and decisions during an incident. The goal is to capture a record of the incident response with the key information that will help you refresh your memory if questioned

months or even years later. It also assists in the audit function and any potential legal actions related to the incident. Good documentation may mean that you do not receive a phone call asking what or why you did something. Remember to record all details for your role in key events, such as injuries/crashes, agreements, and actions.

Protect Personal and Sensitive Information

All ICS staff should use appropriate measures to safeguard and prevent the unauthorized release or unintentional access to personal or sensitive information of both responders and citizens affected by disasters. Sensitive Personally Identifiable Information (PII), if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of PII include Social Security numbers, Alien Registration numbers, financial account numbers, and biometric identifiers (e.g., fingerprint, iris scan). Other data elements, such as citizenship or immigration status, account passwords, and medical information, in conjunction with an individual's identity, are also considered Sensitive PII.

Information protection also includes medical, financial, and other sensitive or classified information that is not subject to disclosure based on legal guidelines. If in doubt, consultation with legal counsel or other governing bodies should be considered.

The context of the PII may also determine its sensitivity, such as a list of employees with poor performance ratings. To protect the privacy of individuals and policies, there should be methods in place to safeguard Sensitive PII when collecting, accessing, using, sharing, and destroying it. For more information, refer to the current version of the Department of Homeland Security (DHS) Handbook for Safeguarding Sensitive Personally Identifiable Information.

For access to the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, go to: https://www.dhs.gov/publication/dhs-handbook-safeguarding-sensitive-pii.

Promote Safety and Security

Ensuring the safety and security of survivors and emergency workers is a fundamental requirement. All staff members have responsibilities concerning risk assessment and safety management. There should be an emphasis on safety guidelines.

Failure to establish and maintain a secure environment will hinder all response efforts. All supervisors and managers should ensure that adequate safety measures are in place and that safety practices are observed. Supervisors are responsible for ensuring that staff follow the safety measures and plans and do not undertake acts that are not within standard guidelines and operating procedures. Routine and consistent briefings should be conducted, and consultation with the Safety Officer should occur when concerns arise.

Manage Risk and Ensure Safety of Your Subordinates

The primary means by which we prevent accidents during an incident is through aggressive risk management. Our safety philosophy acknowledges that while the ideal level of risk may be zero, a hazard-free work environment is not a reasonable or achievable goal. Responders and public safety take top priority, and Incident Management Plans should reflect this commitment. The commitment to be accountable for safety is a joint responsibility of all responders, managers, and administrators.

Remember that hazards are things characterized using nouns (people, places, or things), and risks are things described by verbs (actions or occurrences).

Every supervisor, subordinate, and volunteer is responsible for following safe work practices and procedures, as well as identifying and reporting unsafe conditions. Adhering to this five-step Risk Management Process is a consistent way to practice risk management:

- Establishing situational awareness by identifying hazards
- Assessing hazard potential
- Developing hazard controls and making risk management
- Implementing hazard controls
- Supervising implementation and evaluating effectiveness

The Effective Risk Analysis and Safety program states:

- Do more than repeatedly say, “Be safe out there!” Instead, listen actively, take the information on safety concerns from your subordinates seriously, and demonstrate your seriousness to others by setting a personal example.
- Be an advocate for the “crew resource management” approach where the entire crew is looking and listening for dangerous situations and sharing the information with supervisors. The supervisors must respect, consider, and evaluate the input from the remainder of the crew or unit and determine if a change is necessary.
- Know what is at stake. Do not endanger your life or the lives of others to save property. Be aware of responders who take chances that endanger themselves and their team.
- The strategies, tactics, and actions must be commensurate with values at risk and a thorough risk/benefit assessment. This should lead to an appropriate “risk-based response” for the incident.
- Decisions that follow the approach of what a responsible person would do in the same situation, even in the absence of supporting regulations, are normally upheld in court.
- A Risk Management Plan should include a hazard analysis describing hazards, level of risk, necessary personal protective equipment (PPE), and safety precautions.
- Expect the unexpected by having contingencies and reserve resources in the staging area.

- Seek to be proactive to avoid the need to be reactive.

There are several general and discipline-specific safety guidelines that staff must be familiar with. ICS staff will not be familiar with every discipline; however, they can obtain input and guidance from the Safety Officer, discipline-specific assistant safety officers (e.g., Hazmat, SWAT), division/group supervisors, technical specialists, etc. Numerous guidelines can be helpful resources, including Occupational Safety and Health Administration (OSHA), National Fire Protection Association (NFPA), National Wildfire Coordinating Group (NWCG), and Department of Transportation (DOT).

Monitor Personnel for Fatigue, Stress, and Emotional State

All leaders must attend to the health, safety, and welfare needs of their personnel. Response and recovery operations can be very challenging for the members of an ICS organization. They typically work long hours in a very demanding, dynamic, and stressful setting. For certain incidents, the Incident Command should consider the development of a mental health plan with mental health casualty mitigation measures.

Each member reacts differently to the pressure and stress of the response. If people are tired, hungry, angry, frustrated, or psychologically shaken, they are more likely to take shortcuts, make improper decisions, execute tasks poorly, or endanger themselves or others.

Many times, these conditions may not manifest themselves in outbursts or other behaviors but may be much more subtle. Warning signs to watch for include:

- Signs of physical distress such as rapid heart rate, palpitations, headaches, and tremors
- Becoming irritable or hostile toward others
- Being disoriented or confused and having difficulty with decision-making and solving problems
- Withdrawal from others and loss of interest in activities (Substance Abuse and Mental Health Services Administration (SAMHSA), 2020)

As such, supervisors should monitor their personnel regularly. Supervisors need to determine if there is adequate staffing and support if any members are struggling (e.g., the workload is too high, not properly trained or not enough experience for the position, not enough rest), if the team/section/unit is cohesive and working well together, if deadlines are being met, if products are of good quality, etc.

Supervisors need to ensure that ICS staff get enough rest, take time to eat, maintain good hygiene, and take “mental health breaks” throughout the operational period. Monitor responder work/rest guidance and ensure your team implements appropriate work/rest cycles to avoid cumulative stress and fatigue of assigned personnel.

Lead Assigned Staff

Promote a Positive Team Environment

Emergency incidents create a very demanding, stressful, and sometimes frustrating environment. Typically, the time frame is compressed, and personnel must operate under time-sensitive conditions. At the same time, personnel efforts can be very beneficial to the community and rewarding for the team and individuals.

A tremendous level of interaction and interdependency is needed for the ICS organization to be successful. This effort requires a team culture of shared leadership, teamwork, trust, personal responsibility, coordination, and communications between all personnel. It requires both vertical communications between sections and the command staff as well as horizontal communications up and down the chain of command. The concepts of "shared leadership," empowerment, trust, and "crew resource management" are paramount to success.

Leaders should demonstrate "command presence" by being competent, calm, and confident. Remain positive and inspire and influence your team. Ensure that staff conduct themselves in a professional manner and manage issues when they arise.

For FEMA operations, there is a requirement to establish a safe, inclusive, productive, professional, and respectful workplace that is free of harassment, discrimination, retaliation, and violence. Safe work environments should be free from harassment based on an individual's race, color, religion, sex (including pregnancy), national origin, age, disability, protected genetic information, sexual orientation, marital status, parental status, political affiliation, retaliation, or any other basis protected by law. States, territories, tribes, and local jurisdictions often also have similar requirements. Learn your local requirements. For more information on Federal guidance, see DHS MD 256-01 Anti-Harassment Program.

Build a Team Culture

The term "culture" is defined as the set of attitudes, values, goals, and practices that are shared by a group of people in an institution or organization. Sharing a common culture underpins the development of an effective team.

Cohesive teams work together to complete the mission and concentrate their actions on the common goal. The ultimate goal of achieving synergy is possible only when a team acts in concert within a common frame of reference. The foundational elements of effective team dynamics include communication, trust, healthy conflict, commitment, and peer accountability.

A mission-driven team tends to share these common congruent values: service for the common good, focus on achieving the defined end-state, encouragement of individual initiative, and efforts toward continuous improvement.

Factors that Undermine Team Performance

Numerous factors can undermine team performance. According to one model, there are five factors that can prevent teams from forming successfully or that undermine team performance. (Lencioni, 2002)

Figure 23: The Five Dysfunctions of a Team

- Lack of trust. Trust is the foundation of any successful relationship. If the members of the team do not trust each other, they will not communicate openly.
- Fear of conflict. If trust is not present, people may avoid open discussions of sensitive topics. This can cause back-channel discussions and personal attacks to thrive.
- Lack of commitment. If members have not bought into the team's values or decisions, they will be less committed and less motivated. This can discourage other team members.
- Avoiding accountability. If members are not committed, then they are less likely to feel accountable. They are less likely to go "above and beyond."
- Inattention to results. If trust, commitment, and accountability are not present, individuals are likely to focus on their own interests rather than group results.

Individual Role in Success of the ICS Organization

Each team member shares in the responsibility for the performance, reputation, and success of the ICS organization. The ICS organization manages the incident, and the Incident Command/Unified Command leads and supports the ICS organization. But every team member and their contributions are valuable and essential to the team's accomplishments and success. Consider from your own experience incidents in which a single individual's actions or behavior has either brought great credit or significant disrepute to an organization.

Here are some specific ways team members can contribute to a positive work environment:

Team Interactions

- Treat all team members, responders, and stakeholders with respect and dignity.
- Act in an ethical, moral, legal, and professional manner at all times.
- Do not engage in or tolerate discrimination, sexual harassment, hostile work environment, bullying, hazing, inappropriate actions, comments, and/or language.
- Address inappropriate behavior when you become aware of it.
- Report infractions of policies immediately to your supervisor. If the supervisor is accused of the violation, notify the next higher supervisor.

Personal Behavior

- Do not take alcohol and/or illegal drugs while actively assigned to the incident.
- Do not engage in or tolerate workplace violence, physical confrontations, disruptive behavior, bullying, or hazing.
- Do not post incident details and thoughts on any social media platform without the expressed consent of the Incident Commander or Public Information Officer.
- Do not access inappropriate sites or view inappropriate images/material while on duty and while utilizing team electronic equipment.
- Report any suspected illegal activities.

Performance

- Perform position and job function in a competent manner and accepted standards.
- Ask for assistance when unfamiliar with a task or process.
- Request assistance if an assignment exceeds your ability to complete the task on time or to the expected level of quality.
- Utilize available tools (e.g., job aids, FireScope FOGS, Incident Management Handbook, reference books, and team plans) as memory joggers/checklists to enhance performance.
- Dress in the appropriate team uniform and safety equipment.
- Trainees must actively participate. They will be given opportunities to perform their position functions and work to complete their position task books.

Safety

- Take responsibility for your own safety and accountability.
- Adhere to team safety policies/practices and applicable laws, regulations, and standards.
- Become familiar with Incident Within an Incident Plan, Severe Weather Plan, etc.
- Risk vs. benefit analysis (formal or informal) shall be conducted before every operational or support function in field operations.

- Share responsibility for safety by addressing and correcting unsafe acts or conditions.
- Only operate motor vehicles and power equipment you are licensed/certified to operate.
- Monitor your work/rest cycle in accordance with agency guidance.

Evaluate Personnel Performance

Ensure that staff are evaluated based on established standards of performance and behavior generally based on accepted norms. Specific items to be considered in performance evaluations are IAP objectives, work assignments from the Assignment List (ICS Form 204), adherence to safety standards, and conformance to expected behavior.

It is good practice to review your evaluation of job performance with the individual. To do this:

- Monitor individual job performance
- Evaluate and take corrective action, as necessary
- Respond to requests for an Incident Personnel Performance Rating (ICS Form 225)
- Prepare position-specific performance evaluations that contain objective (fact rather than opinion-based) observations on the performance of the staff member
- Provide supporting documentation for the individual's training/qualifications file

Address Performance Issues and Challenges

When there are performance issues, it is important to face them openly and directly with the member. To accomplish this:

- Identify specific deficiencies and communicate immediately
- Address deficiencies clearly and objectively (but also try to acknowledge areas of success)
- Assess if the deficiency is related to a training issue
- Be supportive of the person while addressing the deficiency
- Intervene when personnel are not being discrete with sensitive operational information
- Provide counseling or corrective action as appropriate

Hold Staff Accountable

Performance standards (such as production rates) are established based on accepted norms and should include clear expectations for subordinates. This is particularly important when going from one agency or jurisdiction to another. Clear and understandable performance standards include:

- Behavior
- Adherence to policies and guidelines
- Operational discipline

Provide Training Opportunities

Often, performance issues may be due to a lack of training. Be supportive of the staff and provide opportunities for training. Furthermore, if available, provide staff the opportunity to work on task books as well as any opportunities for cross-training.

ICS position qualification systems, such as the National Qualification System (NQS), are based on position-specific training, experience at incidents and events, and proper documentation for service in an ICS organization. Depending on the specific qualification system, individuals complete the position-specific training for their respective positions and become "trainees" within the system. A position task book (PTB) may then be given to the trainee so he/she can begin to obtain and document the experience on "allowable" incidents, events, and in some cases, exercises.

Since ICS position qualification systems are "performance-based," trainees can acquire experience through coaching, mentoring, and evaluation provided by individuals that are experienced and qualified in the ICS position. Most qualification systems require multiple training assignments or experiences and positive performance evaluations to become fully qualified.

ICS organizations must consider "succession planning" to help ensure they will have an adequate number of trained and qualified members for deployments. As such, the ICS organization should actively seek training opportunities within their own deployments as well as with other ICS organizations established for incident response. Training can be performed "on-the-job" (OJT) or just-in-time (JIT). On-the-job training is based on the principle of learning by doing. The ICS position trainee learns by performing the job skills of their assigned position during an actual incident. The trainee is mentored throughout the incident by a qualified, experienced member of the ICS organization. This allows the trainee to perform the job functions of the ICS position while getting accustomed to working in the conditions of the incident environment.

Just-in-time training is on-demand training. Members of ICS organizations can learn new knowledge or skills exactly when they need them rather than them being taught in advance. This is a flexible approach to learning and may not be suitable for all situations. Trainees

need access to required information, when they need it, to be successful in learning what they need to know "just in time." (Nikos A, 2018)

Sources for finding information include but are not limited to asking mentors, other members of the ICS organization, position checklist, Field Operations Guides, databases, scanning Quick Response (QR) codes, online platforms, and internet searches.

Evaluate opportunities for meaningful assignments that contribute to position qualification by querying personnel and exploring opportunities for them to learn a new skill.

Personnel can attend training provided by local, state, and Federal agencies that do not focus on ICS. Courses are taught nationwide that can improve personnel's leadership and emergency management capabilities. Examples include the National Domestic Preparedness Consortium, state emergency management agencies, and Urban Area Security Initiatives.

Ensure Accessibility and Inclusion

ICS organizations must operate in remote, challenging, and austere environments and conditions during many deployments. These challenges may occur in the Incident Command Post and other work locations, such as camp (e.g., lodging, personal hygiene), transportation, etc. Working in high-stress environments increases burnout. All personnel assigned to an IMT should be included to improve team cohesion and communication.

Despite these challenges, ICS organizations should provide "reasonable accommodations" to the extent possible to provide opportunities and access for all members. Some ICS positions (e.g., operational positions) have strict physical requirements; however, many positions do not have physical requirements.

ICS organization members, regardless of physical capabilities, can make valuable contributions to the response and/or recovery effort. As such, ICS organizations should provide "reasonable accommodations" to the extent possible to provide opportunities and access for all members.

- Creating an Accessible Environment: People with disabilities and others with access and functional needs are part of every community. Under the Americans with Disabilities Act (ADA), a person with a disability has a physical or mental impairment that substantially limits one or more major life activities that an average person can perform with little or no difficulty, or has a record of such impairment, or is regarded as having such impairment.
- What Does "Access and Functional Needs" Mean? Simply put, people with "access and functional needs" include individuals who need assistance due to any condition (temporary or permanent) that limits their ability to take action. To have access and functional needs does not mean that the individual has any kind of diagnosis or specific evaluation. These individuals include people who live in the community and who live in institutions or facilities, older adults with or without disabilities, children

with or without disabilities and their parents, individuals who are economically or transportation disadvantaged, women who are pregnant, individuals who have chronic medical conditions, and those with pharmacological dependency.

- Refer Accommodation Needs for Resolution: It is FEMA policy to fully comply with the reasonable accommodation requirements of the Rehabilitation Act of 1973. Under the law, Federal agencies must provide reasonable accommodations to qualified individuals with disabilities, except in cases where this would cause undue hardship. This law is generally replicated and adopted in state and local statutes. Thus, ICS Leaders must manage the needs of all responders in this respect. A system must be set up wherein any responder's request for a reasonable need for accommodation should be reviewed and resolved.

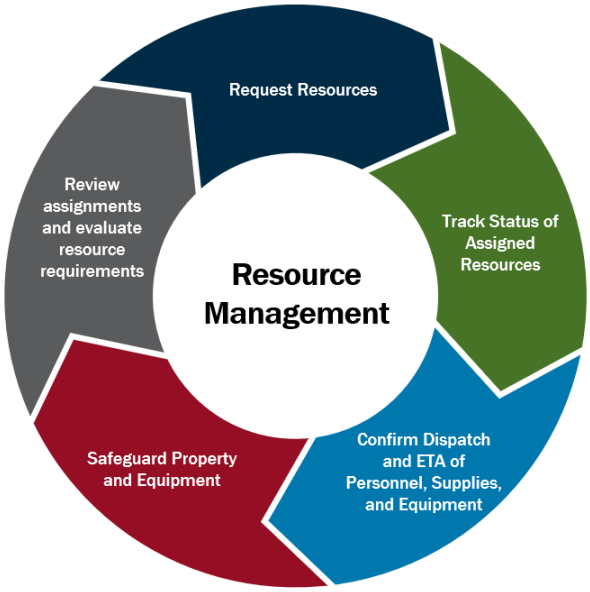
To learn more about Universal Design and Accessibility, go to: https://www.section508.gov/create/universal-design.

Manage Assigned Resources

Resource Management During an Incident

The resource management process during an incident includes standard methods to identify, order, mobilize, and track resources. In some situations, such as when an Incident Commander identifies the precise resources required for a certain job and orders those resources directly, the identification and ordering process is compressed. 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 24: Resource Management Process



Request Resources

ICS leaders must continuously review their assignments and evaluate resource requirements (including staff). When a current or future resource requirement is identified, the leader must communicate this requirement through clearly defined resource requests. When supplies are expended, provide the Supply Unit Leader with a list of supplies to be replenished. Leaders must make every effort to forecast requirements as early as possible because resource availability often lags behind incident resource requirements.

Track Status of Assigned Resources

Each ICS leader is assigned resources to perform their assigned functions. Determining the status of resources starts with the initial briefing via the ICS 201 or verbal briefing from those initial responding units. Once a more formal ICS structure is in place, these duties are assumed by the Resources Unit Leader. While it is the overall responsibility of the Resources Unit Leader to track all resources for the incident, each leader must also understand and constantly update the status of their assigned resources. You should be the most informed person on the incident on the status of your resources. The Resources Unit Leader will derive their situational awareness on the status of your resources from you.

Actions every leader should take for their resources include:

- Maintain resource status information and track assigned resources
- Provide situational awareness of the status of all assigned resources
- Understand and communicate when a resource is no longer required and is available for reassignment or demobilization
- Respond to requests about the status and location of assigned resources

- Contribute to the assigned resource information used by the Resources Unit Leader and the Situation Unit Leader for the Incident Status Summary (ICS Form 209)
- Contribute to the assigned resource information used by the Command and General staff within the team to enable them to complete their assigned tasks

Confirm Dispatch/ETA of Personnel/Supplies/Equipment.

ICS leaders must confirm dispatch and estimated time of arrival of staff and supplies. Check with logistics on the status of resources requested during routine meetings. Try to keep it on a regular basis and refrain from "pestering" them as it only tends to reduce their effectiveness.

Safeguard Property and Equipment

All staff should take proper precautions to ensure that property and equipment are secured and that measures are taken to prevent theft, loss, or preventable damage. It is critical that sensitive and durable equipment and property are properly checked in and accounted for before a resource demobilization and the incident completely being terminated.

Personnel are responsible for safeguarding all property and equipment assigned to them. Responders must have confidence that their equipment is in good condition and ready for use. Inventorying, maintaining, securely storing, and handling equipment properly instills confidence. Responders use equipment to perform the tasks necessary to attain the incident objectives. Failing to follow procedures to safeguard property and equipment could cause delays in executing tactics, and this could, in turn, increase incident complexity.

Chapter 4: Training, Qualifications, and Credentialing

The National Qualification System (NQS) provides a foundational guideline on the typing of personnel resources and minimum standards for position qualification. The NQS supplements the Resource Management component of the NIMS by establishing guidance and tools to assist stakeholders in developing processes for qualifying, certifying, and credentialing deployable personnel, including ICS staff.

NIMS Guideline for the National Qualification System

The *NIMS Guideline for the* National Qualification System *(NQS)* describes:

- The components of a national minimum standard for position qualification
- The process for certifying the qualifications of incident personnel
- How to implement a peer-review process
- An introduction to the process of credentialing personnel

NQS uses a performance-based approach that focuses on verifying personnel's ability to perform as necessary in incident-related positions. This approach incorporates education, training, and experience to build proficiency and establishes performance as the primary qualification criterion.

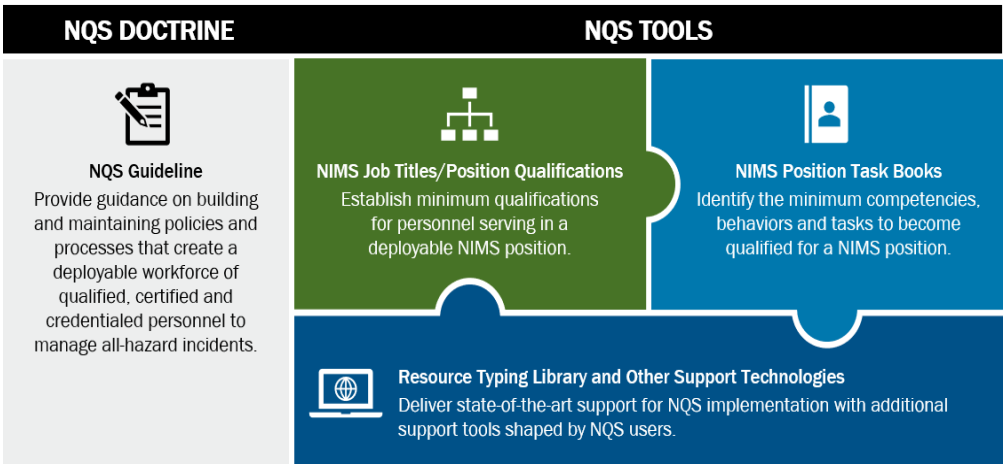
This approach differs from training-based systems, which use the completion of training courses or passing scores on examinations as qualification criteria. A performance-based approach provides greater confidence in on-the-job performance since evaluators have observed the proficiencies of the individual through their performance of a series of pre-designated tasks.

FEMA supports the NQS by providing guidance and tools to assist Authorities Having Jurisdiction (AHJs). (NIMS, 2017)

Authorities Having Jurisdiction (AHJ)

Authorities Having Jurisdictions is the NIMS term for entities that have the authority and responsibility to develop, implement, maintain, and oversee the qualification, certification, and credentialing process within their organization or jurisdiction. Authorities Having Jurisdiction 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.

Figure 25: NQS Doctrine and Tools



- The **Guideline for the National Qualification System** provides guidance on building and maintaining a process for creating a deployable workforce of qualified, certified, and credentialed personnel to manage and support incidents of all types and sizes.
- A set of **NIMS Job Titles/Position Qualifications** defines the minimum criteria that personnel serving in specific incident-related positions must attain before deploying to an incident. These criteria describe not only required capabilities but also specific education, training, experience, physical/medical fitness, currency, and professional and technical licenses and certifications, when appropriate.
- **NIMS Position Task Books (PTB)** identify the competencies, behaviors, and tasks personnel must demonstrate to qualify for specific incident-related positions. PTBs are a standardized tool for observing and documenting the trainee's performance and are widely used by organizations, associations, and governmental entities to qualify incident management and support personnel. Key tools of the NQS qualification process, PTBs:
    - Provide an observable, measurable, and standardized means to document the trainee's proficiency by describing specific tasks, behaviors, and competencies for each position; and
    - Streamline and standardize the evaluation process by enabling evaluators to observe and document the trainee's performance during qualifying incidents, events, job activities, exercises, or classroom activities.

Support Technologies assist stakeholders in implementing effective qualification and certification processes. For example, the Resource Typing Library Tool (RTLT) is an online catalog containing resource-typing definitions, NIMS Job Titles and their corresponding Position Qualifications, and NIMS PTBs. Figure 26: NQS Concept of Operations depicts the continuum of the integrated qualification, certification, and credentialing processes

that constitute NQS. A summary of activities for each of the three processes is described below.

Figure 26: NQS Concept of Operations

- **Qualification** is the process of enabling personnel to perform the duties of a specific position while also documenting their mastery of the skills required by the position. During the qualification process, trainees—individuals seeking to become qualified—meet the prerequisites for the position they are pursuing by completing training courses, obtaining professional or technical licenses and certifications, if appropriate, and meeting the physical and medical fitness requirements established for the position they are pursuing.

Certification is the recognition from the Authorities Having Jurisdiction or a third party stating that an individual has met the established criteria and is qualified for a specific position.

- As part of the certification process, a Certifying Official (CO) and/or Qualification Review Board (QRB) examines the trainee's records of performance and the evidence that the trainee meets all the requirements for the position, including historical recognition, if appropriate. If the trainee meets all requirements, the Certifying Official certifies the individual "qualified" for the position.
- Please note that the term "certification" in the context of the NQS refers to the Authorities Having Jurisdiction certification that an individual is qualified for a specific incident-related position. It is distinct from professional certifications and licenses.

Credentialing is the process of providing documentation that identifies personnel and verifies their qualifications for certain positions.

- Once an individual is certified for a position, the Authority Having Jurisdiction issues an identification card or badge—a credential—attesting to the identity of the individual and his/her qualifications and affiliations. Authorities Having Jurisdiction determines what kind of identification card, badge, or other identification documents to issue.

Examples of credentials include, but are not limited to, the basic Incident Qualification Certification System Card, used by some Authorities Having Jurisdiction who support wildland fire responses, and a radio frequency identification (RFID)-chipped Personal Identity Verification (PIV) card with the capacity to contain significantly more detailed information about the individual.

Recertification is the confirmation that an individual has maintained his/her qualification for the position.

- The Authority Having Jurisdiction maintains records regarding its personnel and establishes procedures for the periodic review of these individuals' qualifications and their current positions. This may result in formal periodic recertification or decertification if individuals no longer meet minimum qualification standards or do not possess the current position's requirements.
- Recertification periods may vary depending on the position. It is up to the Authority Having Jurisdiction to establish the recertification timeframe.

NQS Competencies and Position Qualifications

FEMA also maintains a set of NIMS Job Titles and Position Qualifications that define the minimum requirements that personnel serving in various incident-related positions must meet to be considered qualified for deployment. They describe specific education, training, experience, physical/medical fitness, and professional and technical licenses and certifications required for each position.

For access to all standard NIMS Job Titles and Position Qualifications, visit the FEMA website at: https://www.fema.gov/emergency-managers/nims/components/positions

FEMA also maintains NQS Position Task Books (PTB), which identify the competencies, behaviors, and tasks personnel must demonstrate to qualify for specific incident-related positions. PTBs are crucial tools of the NQS qualification process because they provide an observable, measurable, and standardized means for observing and documenting the performance of trainees during qualifying incidents, events, job activities, exercises, or classroom activities. PTBs are widely used by governmental entities, associations, and other organizations to qualify incident management and support personnel.

For access to all standard NQS Position Task Books, visit the FEMA website at: https://www.fema.gov/emergency-managers/nims/components/position-task-books

Qualification Process

NQS qualification is the process of:

- Enabling personnel to perform the duties of specific incident-related positions and meet any other prerequisites established for the positions; and
- Documenting the fact that individuals have demonstrated the capabilities and competencies required for those positions (NIMS, 2017). Personnel can perform the

duties of a particular position through a combination of training, on-the-job coaching, and experience. One or more evaluators observe, attest to, and document an individual's ability to perform specific tasks as described in PTBs. Individuals may be qualified in multiple positions. An Authority Having Jurisdiction determines how many qualifications an individual can hold at one time.

Examples of qualification criteria include:

- **Performance:** Completing the Position Task Book required for the position.
- **Education:** Formal instruction based on a curriculum that is designed to prepare an individual for a position. It is intended to provide an individual with the core knowledge, skills, and abilities to enter into a discipline and perform job functions.
- **Training:** Courses that must be completed before becoming qualified in a position.
- **Experience:** Being qualified for and serving subordinate and other pertinent positions, measured in terms of time spent applying the specific skills associated with the position.
- **Physical/Medical Fitness:** Physical and medical considerations that, when applied, help to ensure safe performance in potentially hazardous environments. AHJs determine the method of evaluating the physical fitness levels of their personnel; however, the testing method should be a measurable evaluation process.

For example, the role of a Situation Unit Leader can be a high-stress job that requires a great deal of networking and data-gathering to complete position tasks. Many of the forms they use are very specific. Some tasks require mapping skills or the use of various technical tools and software. For that reason, each of these criteria is critical to success and should be considered when determining if a person is qualified for the role.

Position Task Books

Under most qualification systems, the member of the ICS organization must meet required prerequisites and complete position-specific training courses before a position task book (PTB) is opened. The trainee's direct supervisor typically requests the issuance of a PTB to the trainee. Once an AHJ issues a PTB, trainees are required to complete the PTB within five years; however, many positions are typically completed in significantly less time.

The qualification system for ICS staff members is a *performance-based* system. This means that the trainee (person who is attempting to become qualified) must demonstrate proficiency in required tasks or skill sets related to the position. This evaluation must occur during qualifying incidents or events.

The performance of trainees is documented in the PTB by their evaluators. Most qualification systems require the trainee to complete the tasks multiple times at different incidents. When the PTB is completed, it will be reviewed by a final evaluator to ensure the

required tasks have been completed satisfactorily. The PTB will then be forwarded to a Qualification Review Board for a final review and to determine if the trainee has performed successfully and met all the position requirements.

Qualifying Exercises

While trainees demonstrate proficiency in actual incidents, AHJs may also allow trainees to complete certain PTB tasks in exercises. This action can accelerate the qualification process when opportunities for trainees to perform on actual incidents are limited. AHJs should also indicate which tasks their trainees may complete through exercises and what trainees must demonstrate in actual incidents.

Certification Process

Certification is the AHJs final and official documentation. It indicates that an individual is qualified to perform in a specified NIMS position. Certifying personnel helps to ensure they possess a minimum level of education, training, experience, physical and medical fitness, and capabilities appropriate for a particular position. Individual certifications can be listed in various databases used by state/local governments, such as the Incident Qualification System (IQS) or the Incident Qualification and Certification System (IQCS) that many Federal agencies use.

Once the jurisdiction's AHJ determines that a trainee has successfully completed all requirements for a position, the board forwards a recommendation to the AHJ's Certifying Official (CO), explaining its findings and recommending that the CO certify the trainee as qualified for the position. If the AHJ determines that the trainee's package does not provide enough evidence that the trainee has met the requirements for the position he/she is pursuing, the AHJ returns the package to the trainee, along with an indication of any unmet requirements. Acting on the AHJ's positive recommendation, the CO certifies that the individual is qualified for the given position. The AHJ maintains documents regarding the employee's qualification and enters the pertinent information into the AHJ resource/personnel management systems.

Recertification

Certifications are not permanent. AHJs have established a process to ensure that personnel continue to be capable of performing in the position(s) for which they are certified. They typically do this through a process of periodically reviewing and, if merited, recertifying personnel. Recertification periods may vary depending on the position. It is up to the AHJ to establish a recertification timeframe. To prevent the degradation of knowledge, experience, training, and capabilities required to successfully carry out the responsibilities of a position, AHJs typically require a person to perform in that position at least once every five years. However, this period may vary based on the established timelines of the AHJs.

Credentialing Process

Credentialing is an essential final step in qualifying, certifying, and credentialing personnel for incident-related positions. A common nationwide credentialing approach helps to expedite access to incident sites, acceptance of credentials by other jurisdictions, and ideally, the assurance that personnel deploying to other jurisdictions have the knowledge, experience, training, and capability to perform the duties of their assigned incident-specific roles. Being able to quickly and confidently identify incident management and support personnel from different jurisdictions or organizations who are qualified and authorized to perform incident duties is essential to an efficient integrated incident management operation. (NIMS, 2017)

Chapter 5. Information Management

Incident management requires a vast amount of information sharing from the planning stages through response and recovery. Information of all types and classifications is constantly created, collected, shared, and stored in various forms. Mismanagement of this information can have serious consequences. The consequences of not adhering to NIMS, ICS, or other applicable information management standards can lead to:

- Loss of life and property
- Denial or de-obligation of reimbursable funds
- Civil penalties related to lawsuits for not following procedures
- Criminal prosecution for indifference in not following standards or policies

This chapter will discuss the proper handling and management of all types of information.

Information Management Definitions

Data

Data are unprocessed material that may be incorrect, irrelevant, redundant, or, in some cases, actually useful. The Department of Homeland Security (DHS) definition includes the observation that data are "a value or set of values that provides a *representation* of facts, concepts, or instructions in a formalized manner suitable … interpretation, or processing by humans or by automatic means." Data are the facts or details from which information is derived.

Information

When data is processed and presented in a context that makes it useful, it is referred to as information. Data becomes information through the processes of validation (is it accurate) and analysis (is it relevant and useful). Information is further defined by the Department of Homeland Security (DHS) as data in a usable form, usually processed, organized, structured, or presented in a meaningful way.

Information may be based on a single validated and analyzed data element, or it may be a combination of several other validated and analyzed data elements which together have meaning within a specific environment or from a particular perspective. This is called context; the meaning of data can vary according to the context in which it is being utilized. (Management Directorate, Department of Homeland Security, 2017)

Intelligence

Intelligence is a term that holds a variety of meanings in different organizations. Some define it as processed information accompanied by a recommendation. Some use it to refer to information used by the Federal government in classified activities. In NIMS, intelligence is a term referring exclusively to threat-related information developed by law enforcement, medical surveillance, and other investigative organizations. Intelligence normally has special access and handling requirements.

According to the NIMS definition, it is critical to understand the difference between information and intelligence. Validated and analyzed data becomes information. Some of this information, the part that is "threat-related information developed by law enforcement, medical surveillance, and other investigative organizations," is referred to as intelligence. All intelligence is a form of information, but not all information meets the NIMS definition of intelligence.

Intelligence generated and managed within the Intelligence/Investigations function (when implemented within the ICS organization) is information that either:

- Leads to the detection, prevention, apprehension, and prosecution of criminal activities or the individuals involved, including terrorist incidents.
- Leads to determination of the cause of a given incident (regardless of the source), such as public health events or fires with unknown origins. (Management Directorate, Department of Homeland Security, 2017)

Additional Information Terms

Classified Information. United States national defense or foreign relations information designated as classified using categories including Confidential, Secret, or Top Secret.

Sensitive Information. Information that, if accessed or disclosed without authorization, could adversely affect security, ongoing investigations, the conduct of government programs, or the privacy of individuals.

Personal Identifiable Information. Information that permits the identity of an individual to be directly or indirectly inferred.

Classified, Sensitive, and Personally Identifiable Information all have special considerations for handling, storage, and dissemination.

Situational Awareness

Situational awareness is defined here as the ability to identify, monitor, process, and comprehend critical information about an incident. Achieving this requires continuous monitoring of relevant sources of data related to the incident and developing hazards.

Common Operating Picture

A Common Operating Picture is a continuously updated overview of incident information. The Common Operating Picture contains the key information needed to plan for the next operational period, track incident progress toward achieving the objectives, and support decision-making. The Common Operating Picture is shared so that all participating organizations at all locations have a common set of information about the incident. All incident participants benefit from this sharing of critical information. The full Common Operating Picture is not normally made accessible to the media or the public – it is intended for use by incident personnel.

Essential Elements of Information (EEI)

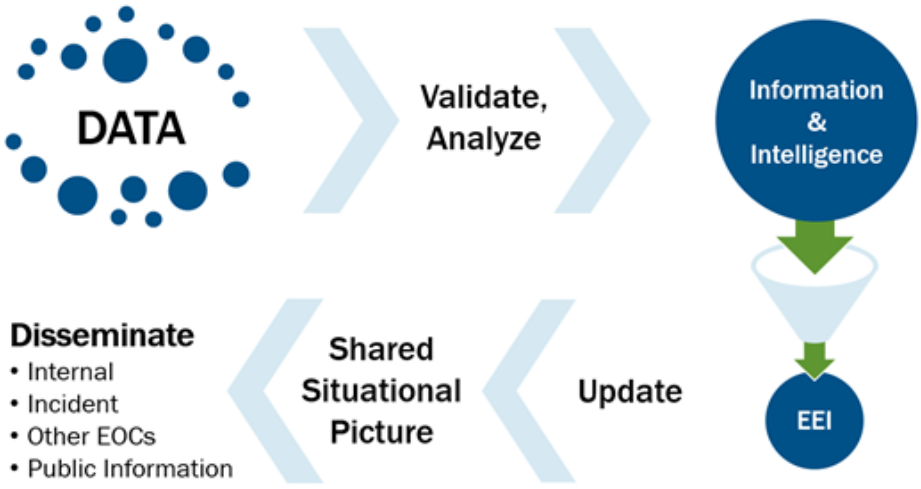
Essential Elements of Information are important standard information items that support timely and informed decisions. Clear identification and definition of EEI ensure that incident personnel gather the most accurate and appropriate data, translate it into useful information, and communicate it with appropriate personnel.

Essential Elements of Information:

- Create a starting point for collecting information
- Contribute to an analysis by defining what information is most relevant to Situational Awareness, decision-making, and Common Operating Picture
- Organize information using defined categories for relevant information
- Define required data elements for the population of the Common Operating Picture and generation of Situation Reports
- Provide context for understanding the situation (Situational Awareness)
- Provide the necessary information for decision-makers to make decisions

Situational Awareness and Decision Support

Figure 58: Visualizing Incident Information



The information cycle begins when data is received. Data is collected on the incident scene or sent to the Incident Command from the EOC and other agencies and sources. The Incident Command staff then verifies that the data is valid/correct and analyzes it to determine if it is pertinent to the situation. Processed data is called information or intelligence. Intelligence is threat-related information developed by law enforcement, medical surveillance, and other investigative organizations.

The Incident Command staff must analyze for filtering (sorting or screening) validated data to convert it into useful information. All information is not equally useful. Using defined Essential Elements of Information provides a method to filter validated and analyzed information. Essential Elements of Information are key information identified for use in managing the incident.

The validated, analyzed, and filtered information is Essential Elements of Information (EEI). EEI provides updates to the Common Operating Picture (COP).

Information is disseminated and updated through a Common Operating Picture. The Common Operating Picture is a common source of incident information for those who have contributed, those who are impacted, and those who may become impacted by the event.

Information is also disseminated to the local Emergency Operations Center (EOC) and through the EOC to other States, tribal, or other neighboring jurisdictions. This may be accomplished through a shared Common Operating Picture display. It may also be conveyed via SITREP.

Developing Essential Elements of Information (EEI)

Decision-makers identify Essential Elements of Information (EEI) to ensure personnel gather the most appropriate data, translate it into useful information, and communicate it with appropriate personnel. It is critical to understand that the information that is collected and disseminated must be targeted at gaining and maintaining a clear picture of the information that is required to manage the incident. It is easy and common for an ICS organization to receive more information that it can effectively manage. It is also common to expend effort to track information that has no identified purpose. Not all data that you may be able to collect, validate and analyze will be useful information. For example, it is possible to track the boot size for every responder. This is data that could be collected, validated, analyzed, and reported. But what decision is this information supporting? If there is not a specific reason that you need the information, it should be screened out as a part of the information management efforts of the ICS organization.

The following sequence of analysis can be used as a tool to ensure the critical information is considered when defining the EEI for an incident. Again, Essential Elements of Information are important and standard information items that incident managers need to make timely and informed decisions. EEIs also provide context and contribute to the analysis and help to update the Common Operating Picture and Situation Reports.

Define each EEI by answering the following questions about the proposed EEI for an incident:

- **Requirement** (what do I need to know)
- **Decision** (what decision will this information support)
- **Decision-Maker** (who needs the information to make an incident-related decision)
- **Stakeholders** (who else may need this information)
- **Limitations** (dissemination, handling, or storage restrictions)
- **Method** (how will the information be disseminated)
- **Collector** (who will collect this information)
- **Frequency** (how often do I need to update this information)

If you cannot identify a specific purpose for the information, it is likely not a valid EEI. It may even be something that you want to make a point of screening out early in your data collection process. To refer back to the earlier example, if you have determined that you have no use for information on responder boot sizes, then it is not an EEI, and you may decide to screen out any data you receive on boot sizes. If data is not screened to exclude information that is not needed, the ICS organization can become overloaded with irrelevant information.

One of the most current uses of EEI is the FEMA Lifelines, which examine the status of critical infrastructure and key resources (CIKR) that can be vital in examining the situation and focusing efforts on restoring those functions.

Here is an example of an EEI for an incident. There is a concern that inclement weather may impact an operation. The Incident Commander, in coordination with key Command and General staff leaders, sets an EEI called "weather," which is defined as any significant change in current conditions or forecast that will impact current/next operational period operations for the incident. The purpose of this EEI is to support decision-making to cease response operations and have shelter in place if faced with inclement weather that will produce an unacceptable level of risk to incident personnel. The Safety Officer helps to define thresholds or decision points for this decision based on risk analysis. The Situational Awareness Unit is identified as the collector for this information, and the National Weather Service is the source of the information. The Incident Commander directs when the updates on the status of weather will be made and that the Incident Commander and Safety Officer will receive immediate notification for any imminent weather conditions that could impact life safety.

Situational Awareness

Good situational awareness must be available to incident management personnel throughout the life cycle of an incident to support timely and effective decision-making. The quality of decisions is directly related to the accuracy and completeness of the information on which decisions are based, and situational awareness is gained from many sources. Site inspections, official reports, media broadcasts, maps, and formal and informal assessments all contribute to the base of knowledge about the incident.

Developing situational awareness requires continual monitoring, verifying, integrating, and analyzing relevant elements of information and developing hazards. At its best, situational awareness provides up-to-date information on the status of people, critical facilities, infrastructure, resources, and the environment.

Situational awareness is a responsibility of all members of the ICS organization. All incident personnel contribute to Situational Awareness by sharing information with the appropriate members of the incident command. Normally you will communicate through the established chain of command unless otherwise specified. This can be done using the ICS 209 or similar situational reporting document to capture critical information that is used by various team members as well as other stakeholders. The Situation Unit and the Resources Unit are two elements of the General Staff that routinely receive, validate, analyze, screen, compile and disseminate incident information.

Situational awareness also requires critical thinking. "Is the information I have important- if so, who needs to know about it?"

Some key Situational Awareness tasks for the ICS organization include:

- Understanding information requirements (Essential Elements of Information).
- Continuously collecting data related to the incident information requirements.
- Validating and analyzing data to produce information (and intelligence).

  - Validate and analyze information before acting. Ensure that the information is accurate and sufficient to support operational decisions. Inaccurate or incomplete information can result in poor operational decisions.
  - Recognize the correct actions to take with information. Look for the unusual information that deviates from the expected. Recognize and analyze information discrepancies before proceeding.
- Ensuring information sharing with any Intelligence/Investigations personnel to gain awareness of information or intelligence they have that may affect non-investigative operations.
- Assessing information collection, validation, analysis, and dissemination task performance.
- Communicating situational awareness to all members of the ICS organization (FEMA, 2015) Information Collection Plan

Information Collection Plan

A well-designed information collection plan is an important tool for incident management. The information collection plan is a matrix of information requirements that is keyed to the incident. This plan also lists sources, units of measure, and schedules for collecting various items. Information gathered based on an information collection plan can aid in the development of incident objectives.

As you will see in the example below, each EEI has a primary collector that is responsible for monitoring changes in the situation that meet an Essential Element of Information requirement. Your position in the ICS organization may be the primary collector for an EEI. It is important to understand that even if you are not identified as the collector for EEI, as an ICS leader, you have a responsibility to understand what the EEI is for the incident and to report EEI through the chain of command or other defined reporting channel.

Table 3: Sample Information Collection Plan

EEI #	EEI Name	Information Required	Collector(s)	Source(s)	Update Method/Time	Remarks
1	Weather	Any significant change in current conditions or forecast that will impact current/next operational period	Situational Awareness Unit	National Weather Service	Live stream forecast on COP/update weather summary hourly	Immediate notification of IC and Center Director for any weather conditions that could

		operations for the incident				affect life safety
2	Casualties	Any changes in numbers and current location/status of dead/injured/missing	Situational Awareness Unit	Operations Section Med Unit EOC	Maintain status on COP/update as changes occur	
3	Key Resources	Status of key, scarce resources - Aeromedical - County Hazmat Team - City Bomb Squad	Situational Awareness Unit	- EOC - Resources Unit		
4	Media	Media attention and reporting on the incident	Public Information Officer	- Media requests and reports - Social media	Track/monitor and update - Media info request status - Media reporting - Social media	

Common Operating Picture Displays and Reports

Situation Reports

The Planning Section produces SITREPs, which are the primary summary of information of the immediately completed operational period. Situation reports address Essential Elements of Information (EEI), as well as other pertinent information of the last operational period. Situation reports are also tied directly to IAPs; reports should reflect the results of IAP work assignments. By reporting the results of work assignments, the Situation Report can inform adjustments to objectives, strategies, or priorities of the coming operational period.

Incident Displays

Incident displays are typically produced by the Situation Unit within the Planning Section. Displays provide a visual representation of the incident and enhance understanding, situational awareness, and common operating picture for ICS organizations and other stakeholders. Various agencies have developed their own preferences and practices for how they display incident information. Refer to the following USCG Situation Unit Leader Job Aid, Section 6.7 – Disseminate Information via Displays as an example.

For access to the USCG Situation Unit Leader Job Aid, go to:
https://homeport.uscg.mil/Lists/Content/Attachments/2916/SITL_JA-MAY20.pdf

Incident Maps

An incident map is an essential tool that identifies key incident facilities, operational boundaries (such as divisions), hazard areas and locations at risk, topographical information, etc. The Situation Unit provides information and is commonly responsible for assembling the physical map. When electronic mapping is utilized, trained GIS personnel may be utilized to produce the map.

Important considerations when preparing the incident map include the following:

- Incident maps should include scale, location of true north, date and time produced, legend for the meaning of symbols, incident organization boundaries (branches and/or divisions, etc.), key facilities, and camps.
- Produce the map for the IAP in black and white to facilitate reproduction.

Additionally, special-purpose maps may also be required for the Common Operating Picture display or attached to the Incident Action Plan. Different agencies use a variety of map symbols and icons; there is no one set of official symbols and icons for incident maps. As an example, Figure 59 lists a variety of symbols drawn from the NWCG.

Figure 59: ICS Map Symbology

SYMBOL	FEATURE REPRESENTED
	Incident Command Post
	Camp (identify by name)
	Helispot (identifier)
	Helibase (include name of more than one)
	Fixed Wing Base (include name of more than one)
[I] [II]	Branches (use Roman numerals)
(A) (B)	Divisions (use upper case alphabetical characters
	Incident Support Base (identify by name)
	Staging Areas (identify by name)
	Hazard/Incident/Origin

Proper Handling of Information

For Official Use Only (FOUO)

The term "For Official Use Only" (FOUO) refers to unclassified information that is privileged, sensitive, and otherwise must be kept hidden from the general public, and for which a significant reason, statutory requirement, or regulatory instruction exists to preclude general circulation. It should be used for handling material that is sensitive but not otherwise suitable for classification. “FOUO” status is not a legally established information security classification level.

Information that has been determined to qualify for FOUO status must be indicated by markings when included in documents and similar material. To promote proper protection of the information, markings must be applied at the time documents are drafted or as soon as FOUO information is added. Documents and material containing FOUO information must be marked. (FEMA DIRECTIVE, 2000)

Sensitive or Classified Information

As previously described, special measures must be taken while handling, storing, and disseminating classified and sensitive information. Normally, members of an ICS organization will not encounter sensitive or classified information. If they do encounter this information, they should safeguard the materials and immediately report the discovery

through the chain of command. Under no circumstances should unauthorized persons view or disseminate such materials.

Incident personnel should be aware that classified and sensitive materials are required to be marked properly. This includes conspicuously marking indicating the overall classification of the materials on the exterior of the materials and each page.

Personal Identifiable Information (PII)

DHS defines "Personally Identifiable Information" or PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. This can include information such as name, address, date of birth, "Sensitive PII" is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. This can include things like a driver's license number, social security number, or personal financial information. Personal Identifiable Information and possibly sensitive PII will likely be encountered during incident response. Incident personnel must avoid collecting PII unnecessarily and must safeguard PII they encounter from unauthorized persons that do not need to know.

Protected Critical Infrastructure Information (PCII)

Congress created the Protected Critical Infrastructure Information (PCII) Program under the Critical Infrastructure Information (CII) Act of 2002 to protect private-sector infrastructure information voluntarily shared with the government for the purposes of homeland security. The 6 Code of Federal Regulations (CFR) part 29, Procedures for Handling Critical Infrastructure Information; Final Rule, published in the Federal Register on September 1, 2006, established uniform procedures on the receipt, validation, handling, storage, marking, and use of CII voluntarily submitted to the Department of Homeland Security (DHS). The protections offered by the PCII Program enhance the voluntary sharing of CII between infrastructure owners and operators and the government. The PCII Program protections provide homeland security partners confidence that sharing their information with the government will not expose sensitive or proprietary data. The PCII Program protects information from public disclosure while allowing the DHS and other federal, state, local, tribal, and territorial security analysts to use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures.

Health Insurance Portability and Accountability Act (HIPAA) Information

You should already be aware that personal health information is entitled to privacy and cannot generally be shared without permission.

The Privacy Rule contained in the Federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA" 49 CFR 164.512(b)), recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information required to carry out their public health mission. The Privacy Rule also recognizes that public health reports made by covered entities (such as public health officials) are an important means of identifying threats to the health and safety of the public. Accordingly, the Rule permits disclosure of protected health information without authorization for specified public health purposes such as preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions.

The described exception is only for the "public health authority." This is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or Territory, or an Indian tribe that is responsible for public health matters as part of its official mandate.

These public health authorities must restrict the amount of protected health information revealed for public health purposes to the bare minimum needed to achieve the public health purpose. Members of the ICS organization are not normally acting as a part of a public health authority. ICS staff do not have the authority to release the personal health information of others and have an obligation to safeguard any personal medical information that they receive during incident response. Use caution when releasing information about injured patients or responders. Officials have a responsibility to protect private healthcare information; only release generic/non-specific information such as gender, age range, non-life-threatening or life-threatening injuries, etc. Statements such as "A female in her 20's, or an adult female suffered non-life-threatening injuries as a result of the accident" are appropriate. Statements such as "25-year-old Ruth Smith of Portersville suffered internal injuries and a fractured femur" are not.

Special Information Requirements for Hazardous Materials (Hazmat) Incidents

Hazardous Materials incidents have special reporting and documentation requirements defined in Federal regulations. As a member of the ICS organization, you may not be the person responsible for making this report, but you still will be handling information and producing documentation for the incident that is used to satisfy these requirements.

Per the Code of Federal Regulations on Hazardous Materials (49 CFR Parts 100-185), immediate notification of a hazardous materials incident is required at the earliest practical moment when one or more of the following occurs:

1. A person is killed or receives an injury requiring admittance to a hospital.
2. The general public is evacuated for one hour or more.
3. A major transportation artery or facility is closed or shut down for one hour or more.
4. Fire, breakage, spillage, or suspected contamination occurs involving radioactive material or an infectious substance other than a diagnostic specimen or regulated medical waste.
5. A release of a marine pollutant occurs in a quantity exceeding 450L (119 gallons) for a liquid or 400 kg (882 pounds) for a solid.
6. A situation exists of such a nature (e.g., continuing danger to life exists at the scene of the incident) that, in the judgment of the person in possession of the hazardous material, it should be reported to the National Response Center even though it does not meet the other criteria.

Each notice shall be given telephonically to the Department at (800) 424-8802. Incidents involving etiologic agents may be made to the CDC at (800) 232-0124. For the content of the report and additional information, refer to 49 CFR Part 171.15.

A written report shall be submitted on a Hazardous Materials Incident Report (DOT Form F 5800.1) for all incidents involving the transportation of hazardous materials unless excepted. Detailed reporting requirements are contained in 171.16.

Per the Environmental Protection Agency, reporting a release or spill in water requires contacting the National Response Center (NRC) at 1-800-424-8802.

If reporting directly to the NRC is not possible, reports also can be made to the EPA Regional office or the U.S. Coast Guard Marine Safety Office in the area where the incident occurred. In general, EPA should be contacted if the incident involves a release to inland areas or inland waters. The U.S. Coast Guard should be contacted for releases to coastal waters, the Great Lakes, ports and harbors, or the Mississippi River. EPA or the U.S. Coast Guard will relay release and spill reports to the NRC promptly.

Interacting with the Media

An Incident Commander/Unified Command public information guidance or policies will follow the policy and guidance of the Agency Administrator and jurisdiction that the ICS organization is serving under. It is important that Incident Commander/Unified Command ask for, understand, communicate, and enforce the Agency Administrator's guidance on public information and interactions with the media and the public.

The designated Public Information Officer is responsible for managing the interactions between the ICS organization and the media. There is a reason for the designation of Public Information Officer in the ICS organization – it is a specialized function requiring special training and skills. If you are the Public Information Officer for your ICS organization, you should have specialized training in performing your position responsibilities, such as the ICS

Public Information Officer Position Training course. If you are not the Public Information Officer, you should understand and follow their guidelines for interactions with the media.

The Public Information Officer will understand that the key to working successfully with the media is understanding their needs and seeking to meet these needs as much as possible within the limitations of law and guidance from the Agency Administrator and the Incident Commander/Unified Command. It is an advantage for the Public Information Officer to know the media (particularly the local media). If you have insight into media personalities, you may be able to help the Public Information Officer by sharing your information and insight, particularly if they are coming from outside the jurisdiction and are not familiar with the local media.

Understand that Public Information Officers have two main functions in working with the media.

- They serve as "chief storytellers" for the agency or agencies managing the incident, especially telling the story of the brave men and women who are risking their lives.
- They serve as advocates for the media to other incident personnel.

If the Public Information Officer asks you to interact with the media, they should provide you with talking points or other guidance. Some examples of guidance for media interactions that may be given by the Public Information Officer include:

- Follow the media guidance provided by the Public Information Officer.
- Be prepared.
- Assume that each news media representative is a professional trying to do his or her best to convey accurate information to the public.
- Tell the truth - media personnel are trained investigators – they will likely discover a lie.
- Keep your commitments and do not promise anything you cannot deliver.
- Avoid speaking for other agencies or other individuals unless approved to do so.
- Don't overreact, and do not become defensive.
- Maintain a calm, courteous, and professional attitude.
- If you do not want something on the airwaves, do not say it.
- Be concise and when you are done answering a question, be quiet.
- There are no comments "off the record."

Social Media Considerations

Social media has become a primary information source for many members of the public and is widely used to obtain real-time information during emergencies and to share data about the disaster in the form of geodata, text, pictures, video, or a combination of these media.

Social media has many applications in incident response:

- Increased situational awareness for incident personnel
- A channel of communication with the public
- Two-way communication between the ICS organization and major stakeholder group

While social media allows for many opportunities to engage in effective communications with stakeholders, it also holds many challenges for members of the ICS organization. There is significant potential for unofficial information to be shared with a very large audience instantaneously. There is also significant potential for misinformation on an incident to be spread. As is the case with any data source, social media data can be inaccurate, incomplete, taken out of context, biased, etc. The ICS organization may derive significant and useful data from social media, but it will also have conducted normal information management activities to validate and analyze social media data to determine what part of it is useable incident information.

Using Social Media

Emergency management organizations such as the local EOC should already have an established presence on social media outlets before a disaster strikes; community members should know where to look for information during the response and recovery phases of a disaster. This can include one or more social media platforms such as Twitter, blogs, Flickr, Facebook, Instagram, YouTube, etc.

Members of the ICS organization should not normally be independently posting to social media during incident response unless authorized to do so. The dissemination of incident information through social media should be a part of the overall information management effort of the ICS organization and should be managed effectively. The Situation Unit and the Public Information Officer are two ICS functions that would be most likely to utilize social media during an incident.

Social Media Drawbacks

Some of the main pitfalls of using social media in incident management centers are:

Incorrect Information. Incorrect information can be caused by situations where the true situation is difficult to confirm. Incorrect information and rumors can also be caused by individuals who wish to create confusion. Here are some examples:

- After the meltdown at the Fukushima Daiichi Nuclear Power Station in March 2011, many rumors circulated regarding appropriate safety precautions, such as whether people should evacuate, the possibility of food and water shortages, and whether there would be additional radioactive releases (this example also illustrates insufficient information).

- During a winter storm in January 2014 in Fairfax County, Virginia, the school system was faced with a slew of fake accounts impersonating official accounts and announcing inaccurate school closures.

Insufficient Information. When information is slow to emerge on the circumstances surrounding an event, rumors can start rapidly. Insufficient information can be a result of several factors, such as: not having clearance to release the data, lack of a designated official for that information, or a belief that information must be complete before release and therefore intentionally withheld. Confusion continues to arise when official channels do not release information fast enough, provide information updates in the right social media and traditional media channels, or the population is unaware of or does not trust the official source for that information. The public will generally follow and amplify official information when they can access the information they believe. This happened after the Nepal earthquake in 2015. When there is a new emerging situation that can be confusing, agencies will open their channels of information (such as a conference bridge for volunteers and partners), which can be critical to avoiding mistakes in information management. (DHS, 2018)

Opportunistic Disinformation. Opportunistic disinformation occurs when predatory individuals attempt to capitalize on a particular event or incident. Opportunistic misinformation generally falls into one of two categories:

- Revenue-generating and financially incentivized
- Malicious and politically incentivized

Revenue-generating disinformation attempts to hijack the attention of social media users from a particularly newsworthy happening and redirect their attention for commercial purposes. A phishing scam or spammer may mimic a pre-existing website and redirect the user to a sales pitch or other ad. This technique is like malware that operates by hijacking a browser and redirecting traffic to an alternate website. Scammers capitalize on a popular hashtag and use click-throughs to boost viewer statistics on a website or encourage the purchase of a specific product or service unrelated to the original hashtag. (DHS, 2018)

For example, an article that circulated after a 2014 Sicilian earthquake to supposedly provide news was referring to a 1908 earthquake.

Outdated Information. Today's media environment relies heavily on being first with information. When crisis rumors start to surface, novice and experienced users alike will scour the internet, often posting images of the initial returns from their search without first verifying the date or accuracy of the data they are sharing. This happens most often with users sharing photos from past disasters and portraying them as the current incident. These false representations can often be believed. The phrase "pictures or it didn't happen" describes the mindset of some social media users. Secondarily, older articles describing a past incident can resurface when reposted, and publication dates are changed automatically through reposting. (DHS, 2018)

Ensuring Personnel Follow Social Media Guidance

During the response, many Incident Commanders/Unified Commands will develop guidelines and policies governing their team's usage of social media. In most situations, an Incident Commander/Unified Command will follow the policies and guidance of the Agency Administrator and the jurisdiction in which the ICS organization operates. It is critical that Incident Commander/Unified Command obtain, understand, communicate, and enforce the Agency Administrator's guidance on social media. Typically, the social media guidance prohibits the posting of pictures and other information to personal social media accounts. There is too much potential for information to be taken out of context, for posts to be seen as insensitive to those affected by the incident, or for misinformation or incomplete information to be shared by incident personnel. Responders are encouraged to provide information to the Public Information Officer so that it can be validated and shared as part of the official public information effort. Communicating relevant social media posts that you receive to the situation unit may also help with situational awareness.

Documentation and Records

Importance of Quality Documentation and Records

Proper documentation is vital to the mission. If in doubt, write it down. Err on the side of too much documentation. In a critical incident, your mind will be dealing with a large volume of information. Even during the response, details can be forgotten, and memories can fade quickly after an incident.

From financial audits to legal inquiries, injury investigations, and after-action case studies - documentation is what supports our ability to accurately reflect what happened. Documentation is the legacy of the ICS organization and the key to reimbursement.

The creation and maintenance of documents and records require organizations to have a procedure in place that manages all aspects of their documentation. Specifically, this procedure should address how to produce and manage documents from creation to archiving, as well as ensuring the efficient functioning of the system. Known as Document Control, this procedure is extremely important since it helps ensure:

- Effective management of the organization’s business processes.
- Proper compliance with legislated requirements.
- Clear ownership and buy-in by affected parties.
- Consistent procedures and timelines for review, revision, and approval of pertinent documents.
- Improved opportunities for procedure adherence and training efficiencies.
- Easily retrievable and accurate records.

Documentation Terms

- **Document.** Information and its supporting media such as any paper or computer file that contains information to be followed (e.g., administrative and technical operating procedures, records, and forms).
- **Record.** A document stating results achieved or proving objective evidence that activities were performed. These are not live documents but rather provide a snapshot in time. For example, a record is a filled-out form or template referenced in a procedure or work instruction. Once filled out, they are not live and are subject to change.
- **Obsolete Documents.** Those documents have been replaced by a new version or are no longer required.
- **Controlled Document.** Defined current documents that are used to plan and/or control any processes or operations that affect the organization.
- **Uncontrolled Document.** Any copy of the organization's-controlled documents that are used for reference purposes only. These documents must bear the marking "uncontrolled copy." Or any paper or computer data file that contains HSEQ MS information to be followed and is not controlled.
- **Master Document List.** An index for controlled documents that define the organization. The master document list usually contains, at a minimum, the title, date of issue, revision date, and location of the document.

Documentation Schedule

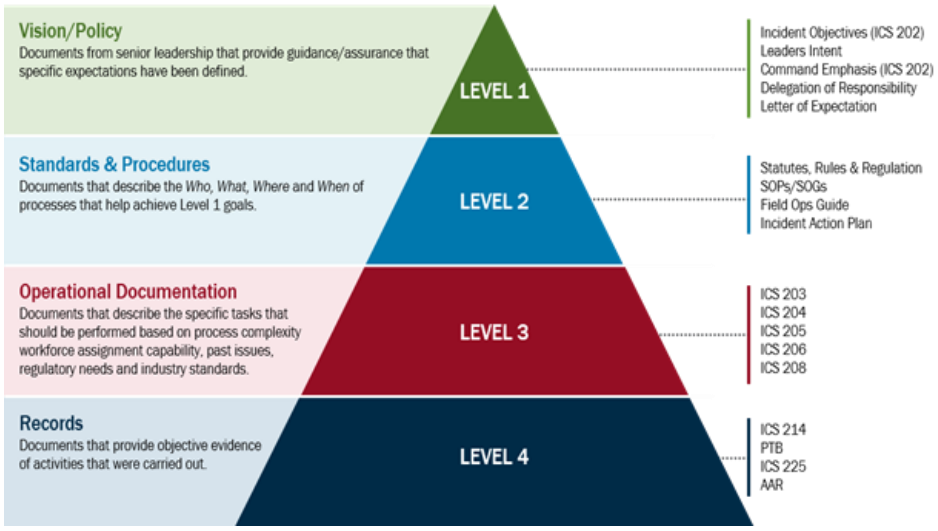
The required documents should be completed on a regular basis and in accordance with a set schedule established by the Planning Section Chief or the Documentation Unit Leader. All supervisors are responsible for ensuring that their staff completes documentation throughout the incident and that it has been reviewed for accuracy and completeness. As all incident documentation generally becomes a legal public document, it should be free from errors and legally signed or noted by the author.

Delay in completing documents tends to cause errors or failure to accurately depict what occurred. In short, our memories fade or become clouded and can obscure our ability to reflect on matters. Remember that you, the author, may be the one using this document much later to refresh your memory of what happened on a certain date in time.

Documentation Hierarchy

The document hierarchy defines the structure with which the organization's management system documents are created. Typically, it is portrayed as a pyramid with each level reflecting the status and quantity of the documents that are typically developed within a well-run organization.

Figure 27: Documentation Hierarchy Pyramid



- Level 1 Documentation – Vision and Policy: These documents are used to provide assurance that senior management has defined and specified requirements/expectations for the organization.
- Level 2 Documentation – Standards and Procedures: These documents include standards and procedures that:
    - Describe the Who, What, When, and Where of the business processes used to meet the requirements of the higher-level policies and Standards
    - Describe the integration of control processes
    - Describe the process flow, linkages, combination, and integration of departments, functions, etc.

  These documents can be created either based on department or by cross-discipline teams focusing on specific elements of the organization.

- Level 3 Documents – Operational Documentation: These documents explain the details of specific tasks or activities – the "how" of performing a specific task and are based upon the complexity of processes, workforce stability, past issues, regulatory needs, and industry standards. These documents must be available, known, and used by personnel and must be kept current and controlled to achieve proper operational performance. Examples include guides, work instructions, plans, forms, drawings, flowcharts, work practices, training plans, and computer templates.
- Level 4 Documents – Records: These documents provide objective evidence of activities that were carried out and the results achieved in accordance with Levels 1, 2, and 3 documentations. They can either be mandatory or implied and they typically include:
    - Individual training needs analyses, records, and assessment results.
    - Calculation results, monitoring, inspection, and audit reports/follow-up.

- Emergency and crisis communication plans.
- Minutes from management and/or committee meetings.
- Communications with administrative and regulatory authorities.
- Incident and emergency reports (immediate, follow-up, final).
- Incident Agency Reports, After Action Report.

Legal Implications and Considerations

Keep in mind that most documents created during disasters or even community events where ICS principles are used are likely to become public documents at some point. Documentation is the official record of what was done and why actions were taken. Documentation protects both the members of the ICS organization and the public.

Ideally, your documentation will demonstrate that you used processes outlined in Federal, state, and local laws and regulations and that you followed accepted standards.

Good recordkeeping is also needed to ensure that any reimbursements from a state or Federal entity have the highest chance of success and the lowest chance of an audit finding.

Some considerations for your documentation:

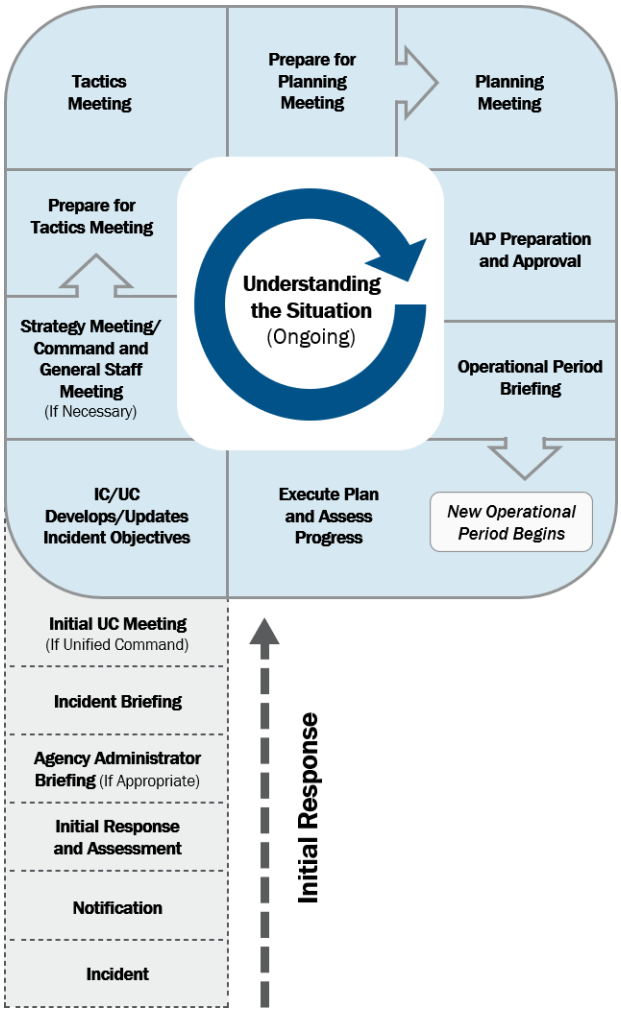
- Are you following relevant laws, regulations, policies, standards, Agency Administrator guidance, and Standard Operation Procedures (SOP)/Standard Operating Guidelines (SOG)?
- Are you systematically documenting significant actions taken in the incident response? This can be done using an Activity Log (ICS Form 214), an electronic events log, or something similar. The adage, “If it is not written down…it did not happen,” is applicable. Another applicable adage is “the strongest mind is weaker than the thinnest ink.”
- Are your files in a logical order? Disorganized files lead to frustration for those who are required to ensure all expenses and actions taken are proper.
- Ensure that you adhere to your state or local record filing and retention regulations. You may need to file documents with your city or county clerk in the permanent official records system.

Chapter 6. Initial Response

The initial response phase includes both preparatory actions prior to arrival on the scene of an incident and response actions that take place en route to the incident scene. The initial response phase may also include preliminary actions taken once on scene. The Operational Period Planning Cycle (Planning P)

The Operational Period Planning Cycle, or "Planning P," as it is referred to, establishes a sequence of meetings and briefings for Incident Action Planning (IAP). You should already be familiar with the Planning P from prerequisite ICS training. In this chapter and the next, we will review the meetings and briefings of the Operational Period Planning Cycle. This chapter focuses on those actions taken during the initial response.

Figure 28: NIMS 2017 Planning P



Variations of the Operational Period Planning Cycle (Planning P)

The National Incident Management System (NIMS) 2017 version of the Operational Period Planning Cycle (Planning P) is shown in Figure 28. There are different versions of the Planning P in use by various organizations. Each version has been adapted based on the experience and practices of the organizations that developed them. Three common variations are those used by NIMS, the All-Hazards IMT Association/National Fire Academy (called the All-Hazards Planning P), and the U.S. Coast Guard. Because the students in this course are training to serve in a variety of diverse ICS organizations, we will try to explain key areas of difference between these different approaches.

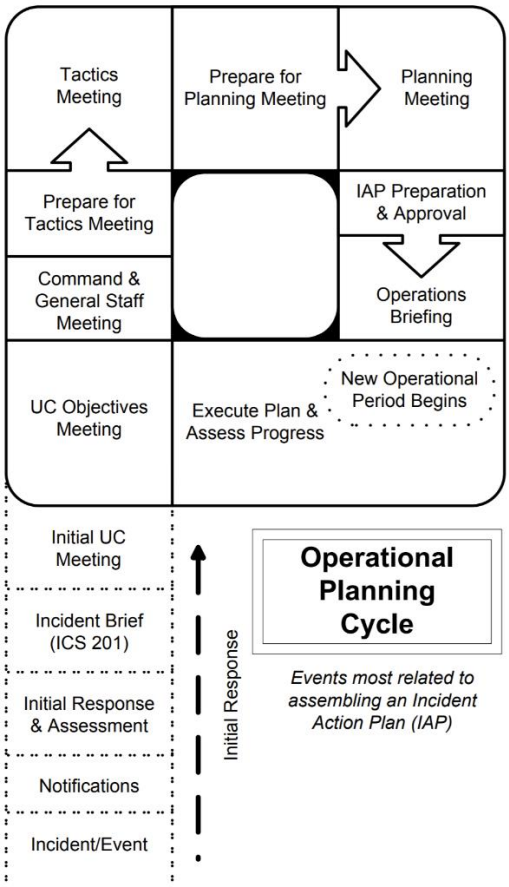
U.S. Coast Guard Operational Planning Cycle

Prior to the Planning P, FIRESCOPE created the Planning Cycle. Over time, it was adopted by the U.S. Coast Guard (USCG), and the Planning Cycle morphed into the first recognizable "Planning P." It was developed specifically to address the operational environment and conditions present when the USCG manages incidents covered by their statutory authority under the National Contingency Plan (NCP).

An image of the USCG Operational Planning Cycle is shown in Figure 29. Key differences between this graphic and the NIMS 2017 Planning P include:

- The USCG model is oriented toward Unified Command rather than Incident Command/Unified Command.
- There is no *Agency Administrator Briefing* step during initial response. This is because the USCG responds under its own statutory authority. This is different from other local, state, tribal, or Federal IMTs that are normally operating with delegated authority from an Agency Administrator to manage an incident. It is important to note that while the USCG Planning P does not detail this meeting, their ICS personnel receives similar guidance such as mission assignment, commander's intent, mission guidance, and authorities from their superiors when they establish a Unified Command to manage an incident.
- The USCG model does not label the Strategy Meeting. However, the description of the activities that occur in the Command and General Staff Meeting incorporates the exact strategy development actions that are included in the NIMS 2017 Strategy Meeting/Command and General Staff Meeting step.

Figure 29: U.S. Coast Guard Operational Planning Cycle



The All-Hazards Planning Cycle

The All-Hazards IMT Association (AHIMTA) is a 501(c)3, not-for-profit professional association comprised of incident management practitioners from multiple disciplines representing Federal, state, and local agencies, nongovernmental organizations, and the private sector. In 2006 The AHIMTA, working with the National Fire Academy and a variety of stakeholders, adapted the USCG planning cycle to better reflect the different legal constraints and operational environments experienced by local, state, tribal (in certain cases), Federal land management agencies, and the responders within the All-Hazards Community.

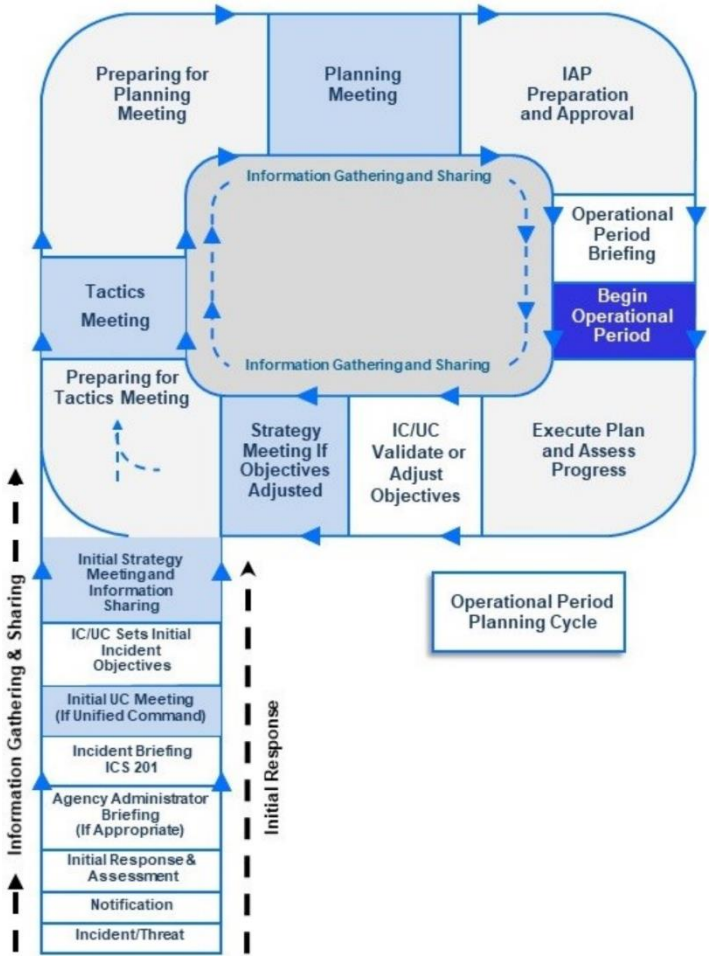
An image of the All-Hazards Planning cycle is shown in Figure 30. Key differences between this graphic and the NIMS 2017 Planning P include:

- The *Incident Command/Unified Command Sets Initial Incident Objectives* and conducts the *Initial Strategy and Information Sharing Meeting* as a part of the Initial Response. In the NIMS Planning P, this is depicted as an activity that occurs at the beginning of Ongoing Operations for each operational cycle. The All-Hazards Planning P does this

during the Initial Response because certain actions taken during the initial development of objectives and strategies are not generally repeated during each operational period.

- The *Command and General Staff Meeting* are not depicted at a set time within the Operational Period. NIMS 2017 depicts this as a step (if necessary) that occurs after Objective development and before the Tactics Meeting. The language of NIMS indicates that this can be referred to as either the Strategy Meeting or the Command and General Staff meeting. The All-Hazards Planning P includes a strategy meeting but does not use the term Command and General Staff Meeting. There can be a Command and General Staff meeting for the All-Hazards approach, but this important meeting is not always conducted at the same time during each operational cycle. The All-Hazards Planning P reflects the common practice that this is a special-purpose meeting that is conducted when necessary, rather than a required meeting that happens as a specific step in the sequence of operational planning events. The key takeaway is that the All-Hazards community treats the Command and General Staff Meeting as a separate meeting, conducted when needed (not at a set time), for different purposes than the Strategy Meeting.

Figure 30: The All-Hazards Planning Cycle



Before Response - Preparing Your Go-Kit(s)

It is recommended that ICS personnel who may be called to fill a role within an ICS organization with little or no notice have a prepared set of equipment and supplies ready in case they are called to respond. This is often referred to as a "Go-Kit." During an incident response, particularly early in an incident, equipment and supplies may not be readily available. Some of these items are for personal comfort and sustainment. Others are items that are required to perform the duties of the ICS position that you will be assigned to. Remember that your Go-Kit will be tailored to your role and to the location and types of incidents to which you will be responding, so some of the items below may not be applicable to your Go-Kit needs. In the position-specific phase of your training, you will receive additional recommendations for your Go-Kit based on your role. The following list provides examples of items that you should evaluate and consider for inclusion in your Go-Kit.

Personal Go-Kit Items

A personal kit should include the supplies and items necessary to sustain one's health and well-being during deployment. This may include:

- Mission-appropriate clothing and sturdy footwear – enough for 14 days
- Hat or other appropriate head covering
- Rain gear and cold-weather gear
- Sleeping gear – bag, sheets, pillow, blanket
- Bathing supplies – towel, soap, baby wipes, shower shoes
- Medications – prescription and over-the-counter – enough for 21 days
- First aid supplies – for minor scrapes and cuts
- Bug spray, repellent, sunscreen
- Food and snacks – enough to supplement the first 72 hours
- Small basic tools – knife, screwdriver, pliers, multi-tool
- Phone chargers, cables, spare battery packs
- Spare glasses, sunglasses
- Small backpack
- Gear bag/luggage – waterproof preferred – able to be carried
- Ziplock bags to pack clothing and other items to keep them waterproof
- Water and/or filtration device

Position-specific Go Kit Items

Items needed for your designated position should include the tools necessary to do your job. Some general categories of position-specific supplies include:

- Essential ICS forms (forms required to prepare the Incident Action Plan to accomplish required reporting) and other forms, documents, and supplies necessary to perform position duties for approximately three days (or up to six operational periods)
- Sample documents, templates, and plans (hard copy or electronic)
- T-Cards and sorter racks: assortment of different T-Cards (100+ of each color)
- Sample Delegation of Authority or Letter of Direction Letter if needed
- Other References such as position job aids, mobilization guides, organizational Standard Operating Guidelines, field operations guide, team guidelines, mnemonics and airport designators, and phone numbers of people you might need to call for more support

Administrative Go-Kit Items

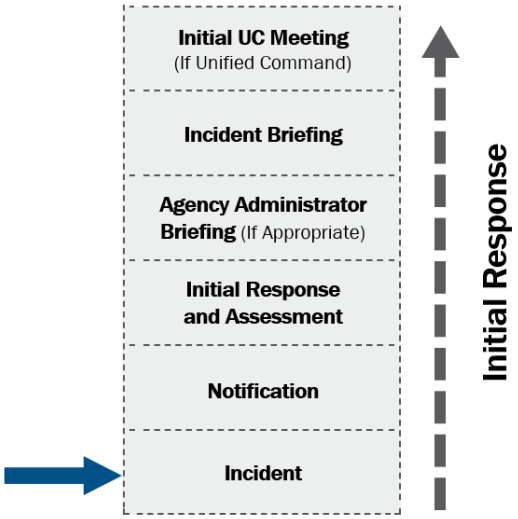
These are general administrative support items that will be needed to perform your position responsibilities.

- Basic office supplies and equipment
- Printer, spare ink cartridges, and printer paper
- Laptop computer (and portable printer/copier) with the following software:
    - Word processing
    - Database
    - Spreadsheet
    - Risk analysis
    - Mapping programs
- Spare cables for laptop computer and accessories
- Data storage devices (flash drives or hard drives) with cables
- Road atlas and/or local maps
- Blue painter tape (3” wide) and/or gaff tape
- Projection equipment including projector with spare bulbs, speakers, cables

Special Response Equipment and Supplies

Depending on the mission and your assignment, some specialized units will require additional supplies or equipment. Mission objectives, strategies, and tactics will determine the equipment needed to address the incident. Most specialized units are familiar with their needs and should be consulted by Command and General Staff on needs to support their missions.

Figure 31: Initial Response: Incident



The initial stages of an expanding incident, as depicted in the Operational Period Planning Cycle (Planning P) diagram, can be compared to the terminology used when an agency transitions from a routine response to one requiring more experienced personnel or the local management team.

This process would be the same for a smaller-sized incident using their local team as it would for an expanding incident where large amounts of resources may be needed for an extended period.

If you follow the steps, you will have a greater chance for a successful and seamless transition.

The initial response to most domestic incidents is typically handled by local "911" dispatch centers, emergency responders within a single jurisdiction, and direct supporters of emergency responders. Most responses will not expand beyond this.

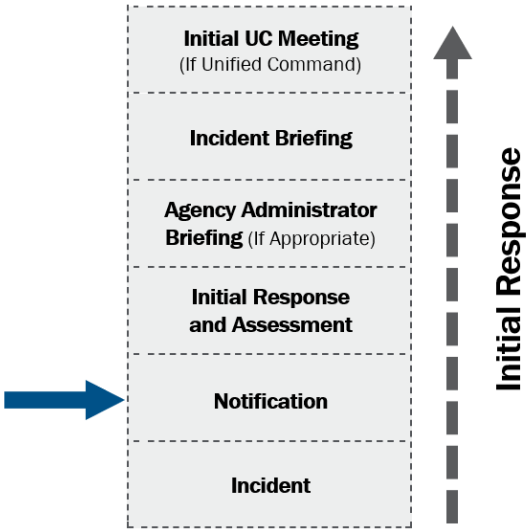
Approximately 95% of all incidents are limited responses that include:

- Command: Incident Commander and other Command Staff.
- Single Resource: An individual, a piece of equipment (and its personnel complement), or an established crew or team of individuals with an identified work supervisor that can be used on an incident.

However, incidents that begin with single resources may rapidly expand, requiring significant additional resources and operational support.

Notification

Figure 32: Initial Response: Notification



The agency becomes aware of the incident and dispatches the initial response resources. This is often accomplished using normal dispatch procedures and following standard operating procedures for first responders.

What to Expect

Do some research on the area where you are being deployed to. What are the local issues on a blue-sky day? What are some of the local customs? Have they been through this type of incident before, or is this an anomaly? As they say, “How big is big and how bad is bad?”

Questions to Ask

Before you deploy, you want to gain as much situational awareness of the incident and mission as possible. Some questions to ask or research may include:

- The basics of what happened and why they need your support.
- What are the conditions on-scene? Do they have basics (e.g., power, water, fuel)?
- What is the status of FEMA Community Lifelines (FEMA, 2020)? This will give you a good picture of what has been affected and the status of the community.
- To whom will you be reporting?
- What is our order number? Resource order number?
- Are there any basic rules and regulations that you should be aware of?

What do we know about the incident?

This question will help you determine the personnel, equipment, and supplies you need to bring. You may need specialized personnel with expertise in certain situations or gear to support your efforts (e.g., you may need to bring a generator if there is no power supply in the area).

Is this a new incident, or am I transitioning in?

This is a critical question as it will determine whether you will have to "start from scratch" or whether there may already be an ICS-type structure in place following NIMS.

Are You Deploying as an Individual or as a Member of a Team?

You may be responding as a part of a pre-designated ICS organization such as a Type 3 IMT that will fill all of the ICS positions. You may also be deployed as part of a smaller group to assist in filling a single ICS function, such as the Planning Section, to assist an ICS organization that has already been established.

Many times, a local ICS organization may be focused on Operations and may lack the resources or expertise for other ICS functions and units. In these cases, they may request a section or unit from another jurisdiction. Also, you could be deployed as an individual to fill a single position to augment an existing ICS organization.

It is important to understand the role that you will be filling and where the other members of the ICS organization are resourced from. This will make a significant impact on what you need to know going into the incident. If you are going in as a part of a full ICS organization that has worked together and has established procedures, you will need to learn and adapt to unfamiliar procedures and possible variations in practice.

Information to Gather Upon Notification

- Incident name and number
- Resource order number
- Agency-specific accounting codes and reporting requirements
- Local government agency or Emergency Operation Center
- Transportation arrangements (drive, fly, etc.)
- Reporting location
- Agency-specific information such as policies and procedures
- Point of contact
- Current status
- Staffing levels on scene for the function
- Lodging (camping, hotel, etc.)
- Who is paying for the travel, lodging, and meals?

- Are you expected to come "self-sufficient" (with your agency or personal credit card), or is the incident providing travel, lodging, and meals?
- If you are expected to use your agency credit card, is your credit limit sufficient?
- Whom do you call to get approval to use it outside of your jurisdiction?

People to Contact

Depending on the position you are assigned, contact with your team leader is critical. From there, you will get your basic information from your dispatch or team. It is important to coordinate contacts and information gathering to avoid duplication of efforts. Should communications be down or diminished in the impacted area, keep in mind that some baseline information can be gathered from open-source data prior to your departure.

Depending on your assignment, you may be able to gain information in accordance with your assignment prior to departure from the following:

- Incident Commander – Current Incident Commander or Agency Representative.
- Operations Section Chief – Local or regional dispatch as well as any other scouting information.
- Planning Section Chief – Local resources for mapping, plans, and other information.
- Logistics Section Chief – Local resources for facilities, staging areas, utility status, etc.
- Public Information Officer – Local media outlets and other information sources.
- Liaison Officer – Maintains contacts for all Assisting and Cooperating Agencies at the incident.

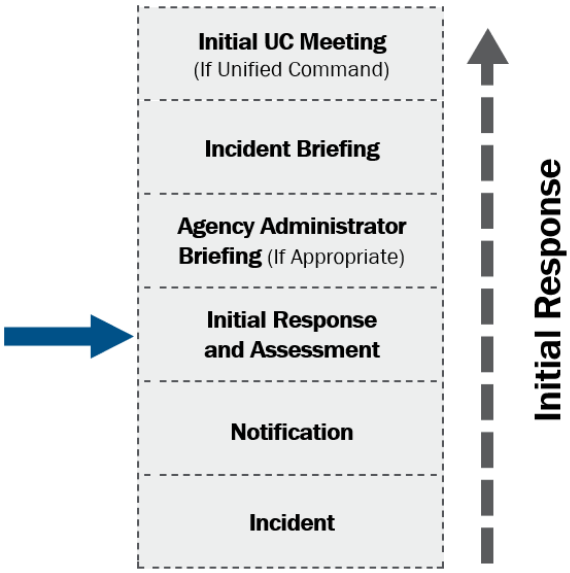
Sizing Up the Incident

Questions to ask may include:

- Nature and the magnitude of the incident
- Hazards and safety concerns
- Hazards facing response personnel and the public
- Evacuation and warnings
- Injuries and casualties
- Need to secure and isolate the area
- Initial priorities and immediate resource requirements
- Reporting location
- Entrance and exit routes for responders
- Weather conditions

Initial Response and Assessment

Figure 33: Initial Response: Initial Response and Assessment



The Initial Response and Assessment step is performed on every incident. However, an incident requiring a full ICS organization will be larger or more complex than you may normally handle in your organization's daily business routine. The application of the ICS organization may be triggered through pre-determined criteria or discussions between the initial responders and the shift supervisors.

During the initial size-up and assessment by the agency and initial resources, if it is recognized that an incident is more complex than normal, a decision is reached to assign a more trained and experienced ICS organization to assume command of the initial response resources. Not every position in the IMT conducts an initial assessment. All members should be familiar with the concept and assist as needed.

For some jurisdictions without an organized local ICS organization of their own, there may be a need to request an external ICS organization, such as a Type 3 Incident Management Team (IMT), to effectively manage the size or complexity of the incident. In some cases, existing policies and laws may influence which ICS organization is utilized for more complex incidents.

Initial Response and Assessment Actions

Actions that normally follow the Agency Administrator briefing are:

- Assessment and Safety
  - Size up the situation
  - Determine if life is an immediate risk

    - Ensure that the safety of all personnel is taken into account
    - Determine if any environmental issues need to be addressed
- Planning and Resource Management
    - Assume command and establish the Incident Command Post
    - Establish immediate incident objectives, strategies, and tactics
    - Determine if adequate resources of the right kind and type are on scene or have been ordered (incident objectives will drive resource requirements)
    - Establish the initial organization that maintains a span of control

Incident Complexity Factors as Part of Size-Up

Obtaining a clear understanding of an incident is critical. Many factors must be considered when performing this assessment, but the most important and all-encompassing factors are situational awareness and incident complexity.

To review, incident *complexity level* refers to the difficulty or resistance faced by incident management personnel while trying to successfully control or manage an incident or an event. Incident complexity is measured on a scale from 1 to 5, with Level 5 being the least complex incident and Level 1 being the most complex.

Incident complexity reflects the combination of factors affecting how severe, widespread, and difficult to control an incident is. Many factors determine the complexity level, including the following:

- Geographic area involved
- Level of threat to life and property
- Political sensitivity
- Organizational complexity
- Jurisdictional boundaries
- Values at risk
- Weather
- Strategy and tactics
- Agency policy
- How routine or unusual the incident is

Determining the level of incident complexity will help the Incident Commander/Unified Command to characterize the incident or event using common terminology. Analysis of the factors that make up the incident complexity will also help:

- Identify hazards and risks
- Determine appropriate objectives, strategies, and tactics
- Identify resource requirements to meet incident objectives
- Determine emergency and incident response personnel responsibilities
- Refine staffing requirements for the ICS organization

NIMS Incident Complexity Analysis Model

The NIMS Incident Complexity Guide provides national-level guidance on assessing and typing incidents based on complexity. The Guide utilizes observable incident characteristics (called indicators) to assist in evaluating and typing the incident complexity. Incident Effect Indicators are observable characteristics seen in damage, consequence, or disruption to the residents, population, infrastructure, and government operations surrounding the incident or event. The Incident Command System (ICS) expands or contracts in relation to the complexity of the incident.

To view the NIMS Incident Complexity Guide, go to: https://www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf

Table 2: Incident Complexity Level: Incident Effect Indicators Summary

Table 2: The NIMS Incident Complexity Guide provides a summary of Incident Effect and Management Indicators that can be used to characterize the Type level of an incident or event. You should become familiar with the more detailed information in this Guide.

Type	Resistance to stabilization or mitigation	How long does it take for resources to meet incident objectives?	Effects on population immediately surrounding the incident	Length of incident effects	Evacuations necessary during mitigation	Adverse impact on CIKR	CIKR impact/mitigation measures	Coordination required with elected/ governing officials and stakeholder groups	Do conditions or actions that caused original incident persist?	Probability of cascading event or exacerbation of current incident
5	None	1-2 hours	Minimal	Minimal	Few or none	None	None	Minimal or none	No	None
4	Low	Several to 24 hours	Limited	Up to 24 hours	Few or none	Minimal	Uncomplicated within one operational period	Minimal or none	No	Low to none
3	Moderate	At least 24 hours	Moderate	Several days to over one week	Possible; may require shelter	Threatens, damages, or destroys property	Adverse; multiple operational periods	Some	Possibly	Medium
2	High	Several days	Significant	Several days to two weeks	Possible; may require shelter/ housing for several days to months	Threatens, damages, or destroys property	Destructive; requires coordination over multiple operational periods	Moderate, including political organizations	Possibly	High
1	High	Numerous operational periods	Significant	Two weeks to over a month	May require shelter/ housing for several days to months	Significantly threatens, damages, or destroys property	Highly destructive; requires long-term planning and extensive coordination over multiple operational periods	High, including political organizations	Yes	High

Incident Safety Analysis as Part of Size-Up

Safety analysis is a core ICS function that must be conducted for every incident. If there is not a designated Safety Officer, the function responsibility remains with the Incident Commander. Even when there is a designated Safety Officer, safety remains a shared function. Regardless of the position you fill in the ICS organization, safety will always be part of your responsibilities. Every ICS leader has a responsibility of understanding hazards, managing risks, and ensuring safety.

When we use the term "hazard" (sometimes called "threats and hazards"), we are referring to something potentially dangerous or harmful. Often a hazard could cause an unwanted outcome such as death, injury, or damage to property and the environment, also called a consequence. The types of threats and hazards are discussed below.

"Risk" refers to the potential for a hazard to produce an undesired outcome. When we characterize risk, the terms "probability" (likelihood of it happening) and "impact" (how significant or serious it will be if it does happen) are used. For example, in February 2021, Texas experienced uncharacteristic extremely cold weather, which caused widespread power outages and rolling blackouts that left millions without power and resulted in 21 deaths. The probability of a cold-weather event of this magnitude in Texas is very low; however, as we witnessed in 2021, the impacts were very high.

Safety starts with a risk assessment to identify potential hazards and to analyze what could happen if a hazard occurs. This is called risk analysis. It is focused on the identification of tactical risks associated with the incident. Once risks are identified, your next step is to consider the actions that can be taken to either eliminate risks or reduce them to an acceptable level. Being aware of hazards, evaluating risks, and seeking to avoid or control risk is critical to the safety of both responders and the community at large.

Threats and Hazards

As a supervisor, you must always be alert to the potential threats and hazards that may impact your operations and staff. In emergency management, there are three categories of threats and hazards: natural hazards, technological hazards, and human-caused incidents.

Everyone has been forced to deal with natural hazards. From floods to droughts, hurricanes to ice storms, every jurisdiction has some kind of natural hazard that can impact their area. Technological hazards and human-caused incidents are easy to get mixed up as both require some kind of human intervention. The way to differentiate between the two is whether there was intent. Technological hazards result from accidents or failures of systems or structures. Human-caused incidents result from the intentional actions of an adversary. In the first case, the incident is accidental. In the second case, it is intentionally done to harm a community.

Below is a breakdown of potential threats and hazards that will help further explain the kinds of problems a responder might face out in the field.

- Natural Hazards
  - **Meteorological** - Flooding, Severe Thunderstorm (Wind, Rain, Lightning, Hail), Tornado, Windstorm, Hurricanes, and Tropical Storms, Winter Storm (Snow/Ice)
  - **Geological** -Earthquake, Tsunami, Landslide, Subsidence/Sinkhole, Volcano
  - **Biological** - Pandemic Disease, Foodborne Illnesses
- Human-Caused Risks
  - Labor Strike, Demonstrations, Civil Disturbance (Riot), Bomb Threat, Lost/Separated Person, Child Abduction, Kidnapping/Extortion, Hostage Incident, Workplace Violence, Robbery, Sniper Incident, Terrorism (Chemical, Biological, Radiological, Nuclear, Explosives), Arson, Cyber/Information Technology (Malware Attack, Hacking, Fraud, Denial of Service, etc.)
- Technological Hazards
  - **Accidents** -Workplace Accidents, Entrapment/Rescue (Machinery, Water, Confined Space, High Angle), Transportation Accidents (Motor Vehicle, Rail, Water, Air, Pipeline), Structural Failure/Collapse, Mechanical Breakdown
  - **Information Technology** - Loss of Connectivity, Hardware Failure, Lost/Corrupted Data, Application Failure.
  - **Industry/Utility** - Dam/Levee Failure, Industrial Accidents, Communications, Electrical Power, Water, Gas, Steam, Heating/Ventilation/Air Conditioning, Pollution Control System, Sewage System.
  - **Fire/Explosion** - Fire (Structure, Wildland), Explosion (Chemical, Gas, or Process failure).

- **Hazardous Materials** -Hazardous Material spill/release, Radiological Accident, Hazmat Incident off-site, Transportation Accidents, Nuclear Power Plant Incident, Natural Gas Leak.
- **Supply Chain Interruption** - Supplier Failure, Transportation Interruption.

There can be a tendency to focus on the primary threat or hazard, such as the overturned tanker with Hazmat, and fail to notice other threats or hazards in the environment, such as power lines or compressed gas cylinders. Look around and think about what other threats or hazards are in the area of operation.

All threats and hazards have impacts. Impacts are the effects of the threats or hazards would have on a community and its responders. This can include responder injuries from exposure to the hazard, vehicle accidents while responding, flammable and hazardous materials present on-site, weather impacts, fatigue, hunger, dehydration, and slips, trips, and falls. The end goal is to reduce these impacts through the use of risk management.

Risk Management

Risk management is a process of identifying potential threats and hazards and analyzing their impacts if they should occur. The first step is to determine what potential threats or hazards exist. Then, assess the probability (also called likelihood) and impacts (also sometimes called consequences or severity in some models). Risks can be ranked based on this simple formula:

$$Risk = Probability\ x\ Impact$$

Once hazards have been identified and the level of risk characterized, the next step is to identify actions that can be taken to manage risk. These are often referred to as "controls." Controls are actions that you take to eliminate (risk avoidance) or reduce (risk mitigation) risk to an acceptable level. As you conduct the risk assessment, look for vulnerabilities (weaknesses) that would make an asset more susceptible to damage from a hazard. These identified vulnerabilities are where your application of controls is most likely to result in a reduction or elimination of risk.

Finally, some risk must be accepted. In any incident, it will not be possible to eliminate all risks. Incident response is normally a reaction to a hazard that has produced an unwanted outcome. Response will involve risk and the goal is to reduce that risk to an acceptable level. Ultimately, the Safety Officer is responsible for the overall incident Safety Assessment, and it is the Incident Commander or the Unified Command that must accept the residual level of risk identified in an operation. However, every ICS leader has a responsibility to understand hazards, manage risks, and ensure safety.

Figure 34 is an example of a tool to assess risk. Each potential hazard is characterized based on its probability and its impact. For example, looking back on the 2021 Texas cold weather incident, the probability of this event happening was very low, but we can see that it had a very high impact.

Think of this in terms of an incident response. If you were part of an ICS organization responding to an incident in Texas, what is the probability and impact of an extreme cold weather event knocking out the power grid while you were trying to manage the incident? The likelihood of this is very low, but the impact would be very high. Using the chart below, this would have been assessed overall as a moderate risk (low probability but high impact). If you put controls in place, such as ensuring that you had access to generators if the power went out, the risk level for your incident response could be reduced to low. By reducing the impacts of the hazard on your operation, you have decreased the risk associated with that hazard.

It is important to understand that risk assessment is done first for each hazard without controls, and then re-evaluated based on the controls put in place. For instance, if I have identified a hazard of moving vehicle accidents during response as high, and I put in place safety controls such as traffic controls and a traffic control plan, I may be able to re-assess the residual risk (risk remaining after controls) as a moderate or even low. The residual risk level is the level that the Incident Commander or Unified Command must accept.

Figure 34: Risk Assessment: Probability and Impact

Probability	Very Low Impact	Low Impact	Medium Impact	High Impact	Very High Impact
Very High	Moderate	Moderate	High	High	High
High	Low	Moderate	High	High	High
Medium	Low	Moderate	Moderate	High	High
Low	Low	Low	Moderate	Moderate	Moderate
Very Low	Low	Low	Low	Low	Moderate

Safety Planning Considerations for all Leaders

When planning for the safety of your team, you should:

- Make sure your subordinates understand their individual and crew responsibility for safety. Do more than just say, “Be safe out there.”
- Listen actively and take your subordinates’ comments and feedback seriously. Take immediate action to address safety concerns from incident personnel.
- Understand the consequences of your actions or inactions. Do not endanger your life or the lives of others unless the benefits and values at risk warrant it.
- Act on anything that feels or appears hazardous.

- Ensure that your personnel have clothing for inclement weather and PPE to provide protection from hazards.
- Attend to personnel welfare needs. If people are tired, hungry, angry, frustrated, or psychologically shaken, they will be more likely to make rash decisions. Make sure everyone on your team had adequate food, liquids, rest, and rehabilitation.
- Ensure a critical incident stress debriefing for critical incidents such as a responder's death.
- Look for responders taking unnecessary or inappropriate chances and needlessly endangering themselves and their team. Take action to address this behavior.
- Set the example by following safety controls and wearing appropriate PPE correctly.

Safety Interactions with other ICS Staff

As you work to avoid or minimize risks and hazards, you will find yourself interacting with a number of other ICS positions, including:

- Liaison Officer - may provide agency-specific operating procedures, limitations (e.g., training equipment), work/rest requirements, and other information.
- Agency Representative - assists with assignments, logistics, personnel issues, specific capabilities, limitations, etc.
- Situation Unit Leader - provides maps with Safety Zones and other pertinent information identified and may also provide up-to-the-minute weather forecasts.
- Geographic Information Systems - verifies the accuracy of maps and may provide SPOT weather forecasts.
- Food Unit Leader - ensures adequate water and hydration, ensures food has the correct number of calories and is safely packaged.
- Technical Specialists

Anticipating Potential Incidents within Incidents (IWIs)

Not all hazards can be anticipated. As in any situation, you may experience events for which you have not planned nor expected those impact incident operations. These are called special situations or incidents within an incident. Examples could include:

- Unanticipated release of hazardous materials
- Unaccounted for employees
- Serious injuries or fatalities

As a leader, you must be prepared for an incident within an incident during response. In some cases, depending on your ICS position and experience level, you may be tasked with assuming command of an incident due to the special situation occurring. In both cases, there is a requirement to manage both current operations and the incident within the incident.

Ideally, the ICS organization has planned for the possibility of an incident within an incident in their response, and this plan can be implemented. Management of the special situation is normally delegated to a Deputy or a senior Section Chief who is supported by appropriate staff.

The Agency Administrator or Executive, appropriate stakeholders (i.e., family, home unit), and investigators/regulators must be notified as quickly as possible. Follow the steps in the emergency plan to ensure all critical items are addressed.

The management of a special situation is called crisis leadership, and this requires a very strong command presence, leadership, and management skills. At the same time, leaders must understand that these crises cause significant human impacts, particularly if a serious injury or fatality has occurred. Leaders must account for this human reaction to an unexpected crisis and display empathy and compassion.

Arriving at the Incident

Check-In

Normally, someone will be on-scene before your arrival, and, at a minimum, they should have established an initial Incident Command structure. The existing on-scene ICS organization should define the check-in location prior to your arrival. If there is a staging area established, this will frequently be the check-in location. However, be prepared for situations in which no check-in has been established. It may become the responsibility of the incoming Incident Command organization. Remember that although critical resources may sometimes be directed to skip traditional incident check-in and report directly to a tactical level leader, members of the ICS staff should always follow a check-in process prior to assuming their responsibilities.

Completing Incident Check-In List

Once you have determined the check-in location at the incident, determine if the incident is using a standard Incident Check-In List (ICS Form 211). If you are responding as a member of a pre-determined ICS organization such as an IMT, you may be able to pre-fill this form for the entire team to streamline the check-in process. In this circumstance, the lead for your ICS organization may be able to process the entire team and avoid congestion at check-in.

You should be prepared to have key information available for check-in, such as:

- Position credentials (if your organization uses a credentialing system to verify position qualification)
- Personal identification (driver's license or other ID)
- Vehicle information, license plate, mileage, make/model

- Resource Order number that you were deployed under
- Demobilization date (if determined by policy or SOP)

Continue Incident Size-Up

Previously, we discussed initial incident size-up activities, including gathering information, assessing incident complexity, typing the incident, and assessing safety concerns. These are not one-time actions. As additional information on the incident is received and analyzed, there should be a continual reassessment of how this new information impacts the size-up of the incident. Does the new information affect the complexity of the incident? Are there new safety concerns that you need to deal with? Reconsider the size-up of the incident as you receive updated information.

Assess Status of the On-Scene ICS Organization

In supporting a new incident, your team may need to consider the following:

- The incident will not be stabilized and may increase in size and complexity.
- All local efforts have been focused on operations with no resources or focus on any supporting ICS structure. Your job may be to bring that structure to life.
- There may have been no formal check-in resources beyond the normal dispatching system in place. Assistance may be needed to set up a formal system.
- Documentation may be lacking. Assistance may be needed to set up a good documentation process.
- Logistical support may be running short. Typically, local response units may start to run low on supplies after a period of time. They may not have experience ordering, managing, and receiving large amounts of supporting resources.
- Responders may be fatigued and/or themselves victims of the disaster.
- Planning needs to begin for the next operational period.

Identify Requirements During an Initial Response

Determining Resource Needs

Prior to responding to an incident, team leaders must examine the situation and determine which resources are required to best meet the needs of the requesting agency. Good situational awareness is key to making these determinations. Many factors, including pre-existing SOPs, will influence whether you need to deploy a "scout team" first to gather good information on the incident, or if you deploy a pre-determined team of resources. Many times, local efforts may need assistance in specialized areas or support functions of incident command.

As you arrive and gain additional situational awareness of the incident and the current ICS organizational structure, you will need to continue assessing the staff and resources

necessary to perform your assigned role. You should identify requirements early because it can take time to procure additional resources and support.

Assessing Existing Resources

Assessing existing resources generally falls into two categories: the status of Community Lifelines and the status of available local resources.

Community Lifelines will offer you a better understanding of how a community's fundamental infrastructure is affected. This will not only tend to drive the objectives in response and recovery, but also will impact the resources available to your team. For example, a lack of electrical power will affect almost every part of the community and would necessitate that your team is prepared to operate without power or bring your own generator capability.

The second category deals with the status and availability of local resources. Do locals have staffing for positions but need some assistance, or do they lack staffing altogether as they may have been victims of the disaster themselves? Many times, local resources have been overworked while responding to the incident, and your team may take over the majority of operations. These are factors that you need to determine to assemble and prepare the right team and resources.

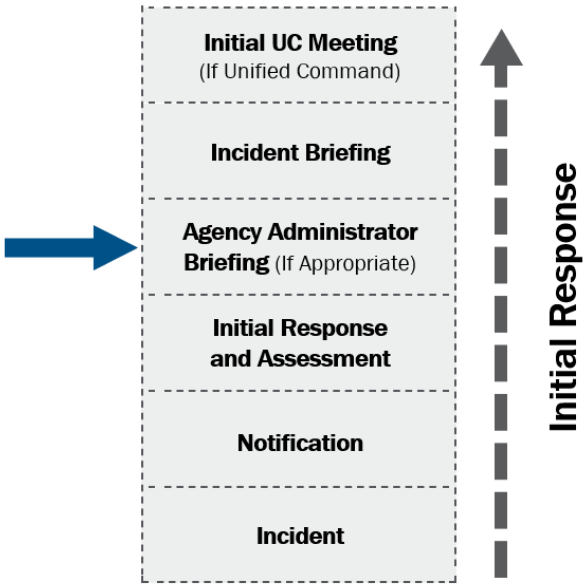
Ordering Needed Resources

You need to understand the process for ordering resources not only to support your team but to be aware of how local resources are ordered as well. If you are sent by your state agency, how do you order more support? Or are you reliant on local ordering systems? These are vital questions that should be discussed prior to arrival or as soon as possible after receiving your briefing from the Agency Administrator or Incident Commander. Utilizing the General Message (ICS Form 213), Resource Request Message (ICS Form 213RR), or similar document/system is recommended for properly managing resource orders and having an acceptable system in place for documenting resource management.

Attending Initial Response Meetings

Agency Administrator (AA) Briefing

Figure 35: Initial Response: Agency Administrator Briefing



The Agency Administrator briefing provides information, guidance, direction(s), and even constraints necessary for the successful management of the incident. A large amount of information is provided during the briefing, and these must be sorted, analyzed, prioritized, and shared among the members of the ICS organization.

Variations in the Planning P

Both NIMS and AHIMTA versions of the Planning P include an Agency Administrator Briefing step. The USCG Planning P does not include this step. This is because the USCG normally manages incidents under its own statutory authority, while most other ICS organizations will manage an incident under authority delegated to them by the Agency Administrator.

Purpose

The Incident Command System (ICS) uses the term “Agency Administrator” as a generic title for the Agency Executive or Official (or designee) who is responsible for that agency’s response to an emergency. This title is used temporarily, regardless of that person’s normal position title. This individual will be a representative of the Authority Having Jurisdiction, also known as the AHJ, and generally, they are the entity that holds legal or legislatively established responsibility for the incident.

The NIMS 2017 Version of the Planning P indicates that the Agency Administrator Briefing may not be required in all incidents. For example, if the incident is law enforcement based (e.g., an active shooter incident), the Police Chief already has statutory authority and policies within the jurisdiction. As such, a briefing with the Agency Administrator is not necessary. However, if the Police Chief is tasked with managing all recovery efforts after a flood, he/she does not have statutory authority over Public Works, Public Health, Fire Department, etc. As such, it would be appropriate to have a briefing from the Agency Administrator to determine their priorities, direction, constraints, etc.

The Agency Administrator meeting is only necessary when:

- The Incident Commander assumes incident management duties outside their normal position description.
- The ICS organization is from a jurisdiction that has not given its local ICS organization pre-established or standing authority to manage the type of incident they are being assigned to.
- The incident exceeds the capability of the agency's normal response organization, and an ICS organization from outside the jurisdiction, such as a Type 3 IMT, is being assigned.

Along with a Delegation of Authority, the Agency Administrator Briefing is used to convey critical information that the ICS organization needs to safely and efficiently assume command of the incident and achieve the management goals and objectives of the Agency Administrator.

In those cases, the incoming Incident Commander must be granted that authority by an official responsible for administering policy for the agency, or jurisdiction, depending on the laws of the jurisdictions involved. In times when the Agency Administrator is legally prohibited from formally delegating their sworn duties, we use terms such as "letter of expectations" or similar documents to convey what the Agency Administrator wants to be done and any guidance or restrictions for the Incident Commander.

To restate key points, the purposes of the Agency Administrator briefing include to:

- Provide a common understanding between the Agency Administrator or Executive and the ICS organization
- Inform the ICS organization of the history and current status of the incident and actions taken to date
- Present the Delegation of Authority (if applicable)
- Present other documents providing information
- Identify key agency personnel who will be involved with the ICS organization, such as the Agency Administrator's Representative
- Establish procedures and schedules for communication and resource ordering

- Establish how news media, public information, and important local and political contacts will be handled on the incident
- Identify special safety awareness concerns and expectations

Participants – Who Attends the Agency Administrator Briefing

At a minimum, the Command and General Staff should attend. Attendance of other members of the teams should be at the ICS organization's discretion. The Agency Administrator's Briefing is not a public meeting; news media should not be invited.

Sharing Information

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 that the jurisdiction, agency, or organization and the incident personnel have a common understanding of the environmental, social, political, economic, and cultural issues relevant to the incident and its location.

Do not confuse this with the practice of notifying an agency administrator or departmental representative of an incident in the community. This is generally part of the SOP for different agencies. We commonly say, "Would you wake up the Mayor or Chief for this incident?" Again, those steps need to be followed, but this segment is talking about receiving a more formal briefing after the Agency Administrator has been briefed and they are given your direction.

The Incident Commander must also be aware of authorities, policies, and external stakeholders as part of the incident size up.

Agency policy can affect the incident objectives. All agencies develop policies and guidelines for accomplishing their responsibilities. The Incident Commander must be fully aware of agency policy, including any limits of authority.

For the majority of incidents, agency policy is known by the Incident Commander because the incident occurs in his/her jurisdiction. These guidelines and policies may be for routine activities or emergency activities, or both. These policies and guidelines may come to bear in the management of an incident, or a planned event based upon the jurisdiction of an agency. For larger incidents, some agencies will require agency policies in writing.

These policies, guidelines, and authorities may give direction on the following:

- Safety
- Operational/control objectives or constraints
- Cleanup and rehabilitation guidelines
- Spending
- Resource sharing

External stakeholders are those parties that are not directly affected by the incident but could be affected by decisions that are made in conjunction with the incident. External stakeholders can usually be identified when the question is asked, "Who else could be affected by this decision?"

Considerations for Transitioning into an Ongoing Incident

If transitioning into an ongoing incident, look for the Incident Status Summary (ICS Form 209), which provides basic information on the current status of the information. The Incident Status Summary is typically obtained at the Agency Administrator Briefing. If you are transitioning with an IMT, expect an Incident Status Summary. An IMT will normally complete an Incident Status Summary for the operational period that has just ended, thus the title Incident Status Summary. They would initiate it once they engage in the incident. If you are transitioning with the initial response, it is more likely that the Incident Status Summary was not completed.

Policies and Guidelines

The following are examples of agency policies and guidelines that can affect the management of an incident:

- Pre-incident plans
- Standard operating procedures
- Emergency operations plans
- Continuity of operations plans
- Community preparedness plans
- Mutual aid and assistance agreements
- Wildland Fire Decision Support System (WFDSS)
- Wildland Fire Implementation Plan (WFIP)
- Corrective action plans
- Mitigation plans
- Recovery plans
- Tribal, State, regional, and national mobilization guides
- Field operations guides
- Delegations of authority

Each member of the ICS organization that participates in the Agency Administrator briefing must effectively glean the information required for that person's functional area as well as issues that span more than one function. Not everyone will "hear the same thing" even though they are listening to the same briefing. The following are some examples of such information:

- Issues, concerns, and/or tasks that affect your functional area.
- Issues, concerns, and/or tasks that are discussed about your functional area but are important to another function. You must ensure the leader of the other function is aware of the issue.
- Issues, concerns, and/or tasks that are discussed about another functional area and have a significant impact on your area. You must ensure that the other team member is aware of the impact on your function.
- Issues, concerns, and/or tasks that may be important when developing Incident Objectives, Strategies, or Tactics.
- Constraints, legal issues, opportunities, or problem areas that affect your function as well as other functions.
- Issues, concerns, and/or tasks that are unclear and will need follow-up or clarification to effectively accomplish the task or deal with the issue.

Sample Agency Administrator/Executive's Briefing Checklist

Incident Name: _____ Incident #: _____ Date _____

Agency Administrator/Official: _____ Incident Commander: _____

- ☐ Incident Description (Incident Status Summary, ICS Form 209) & IAP
- ☐ Incident Summation & General Information
- ☐ Location/Population Affected
- ☐ Organization Charts (Incident Briefing, ICS Form 201)
- ☐ Threats (current/immediate)
- ☐ Political & Community Concerns
- ☐ Financial Considerations
- ☐ Jurisdiction Participants
- ☐ Regulatory/ARARs Considerations
- ☐ Response Options/Proposed Actions
- ☐ Resource Needs (e.g., Contractors)
- ☐ Policy Issues
- ☐ Stakeholders (Who are they and have they been notified?)
- ☐ Priorities
- ☐ Key Issues
- ☐ Health/Safety (includes H&S Plan)
- ☐ Schedule (Assume Command? IC Briefing? Planned Public Meeting? etc.)
- ☐ Management Objectives, limitations, or constraints
- ☐ Visuals (maps, photos, etc.)
- ☐ Need for Inter/Intra-Agency Support
- ☐ Media Interest? How to handle release of information (Agency or IMT?)
- ☐ Technical Data/Monitoring Information Availability and Location
- ☐ Local and Residential/Businesses Affected (area & degree)
- ☐ Other Available Resources (water plans, city equipment, etc. and location or method of obtaining)
- ☐ Community Relations Issues (fact sheets)
- ☐ Deficiencies in Information – Data Gaps
- ☐ Other Command Post Locations or Facility Recommendations?
- ☐ PRP and Enforcement Information
- ☐ Special Information on Finance/Administration (burn rates, source of money, in-kind services ceilings)
- ☐ Reporting requirements
- ☐ What Briefings, to whom it was/will be delivered, Media Interests, and Briefing Schedule
- ☐ Scope of Work (as defined) (Action Memos, Delegation of Authority, Mission Assignments)
- ☐ Logistics Concerns and Needs

Delegation of Authority

Purpose and Contents of a Delegation of Authority or Letter of Expectations

The purpose of the Delegation of Authority letter is to specify the duration and limits of the ICS organization's authority, including fiscal limitations, and to set target completion or commitment timeframes. It may come from an Area Command, Agency Administrator or Executive, or Agency Head. It may be written or verbal.

Not every incident will involve a delegation of authority. In some cases, an IMT may be operating within its own jurisdiction under pre-existing authority given by the laws, policies, or guidelines of the jurisdiction. In these cases, the IMT has been given their authority before the incident occurred as this is part of the established operational procedures of the Authority Having Jurisdiction.

Delegation or expectations should contain at a minimum:

- Responder and public safety
- Tactical constraints: resources and technology available, weather, topography, physical and chemical properties of the material involved, etc.
- Geographic limits: inaccessible areas, jurisdictional boundaries
- Monetary constraints: cost-effectiveness of tactical resources, funding sources
- Timeframes: the urgency of control
- Natural resource risks: endangered species, high value, or high interest
- Social concerns: human life, historical areas, evacuations, air quality
- Potential of secondary target or secondary device
- Political concerns: multiple jurisdictions, demographics, infrastructure
- Economic considerations: effect on the local economy, regional economy, commerce
- Downstream consequences of actions or unplanned results (i.e., containment failure)

Sample Delegation of Authority

Below is a basic template for a delegation letter that can be modified as necessary.

Date:

To: _____, Incident Commander

Subject: Delegation of Authority

As Incident Commander, you are hereby delegated full responsibility and authority for *insert incident type* activities within the *Insert Incident Name* perimeter.

I expect this effort to be conducted in accordance with the Incident Strategic Analysis, which will be reviewed by you and your Incident Management Team.

All available mitigation methods are authorized.

Your main objectives are:

Protect Life, Property, and the Environment
Responder Safety.

Cost expenditures should be commensurate with values at risk.

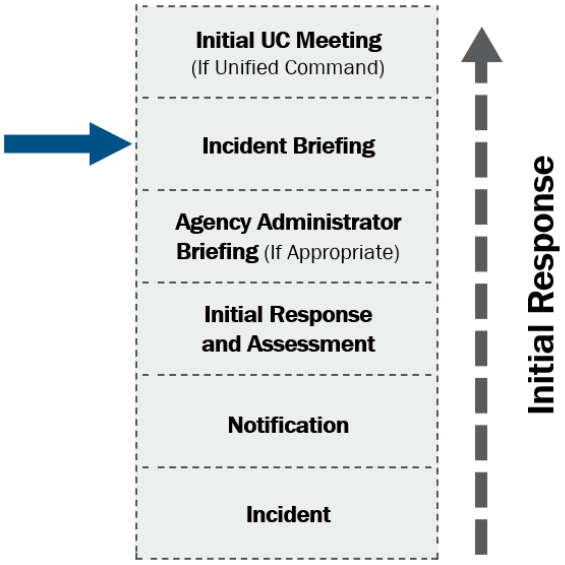
As much as possible, utilize local personnel in training positions or elsewhere in your organization.

_____ of my staff will be my main contact with you. They are authorized to speak for me in the event an administrative decision is needed.

/s/_____
Agency Administrator

Incident Briefing

Figure 36: Initial Response: Incident Briefing



Purpose

Following the Initial Response and Assessment and the Agency Administrator Briefing, an Incident Briefing is conducted using Incident Briefing (ICS Form 201) or a similar tactical worksheet or document. Many agencies maintain this information in their Computer Aided Dispatching System (CADS).

Once the decision is made to assign the incoming ICS organization, or even a higher qualified Incident Commander, the first Incident Commander must start preparing to transfer command to the incoming Incident Commander.

The incoming Incident Commander needs to understand the incident and respond well enough to take command. For example, they should already know the incident situation, response organization, deployed and ordered resources, overall goals, initial response objectives or priorities, and developing objectives. Incident information gathered may also include:

- Type of incident
- Incident history
- Situation Summary and Health and Safety Briefing
- Incident Magnitude, potential, and the estimated duration
- Current and Planned Objectives
- Current and Planned Actions, Strategies, and Tactics
- Current Organization Structure

- Resource Summary
- Resource Assignment
- Resources in-route or ordered
- Political, environmental, and economic constraints
- Status of communication
- Facilities already established
- Locally generated response actions or plans
- Current plan, priorities, and objectives
- Contingency plans (if developed)
- Previously developed sampling plans, site assessments, and data
- Area and facility plans
- Command structure
- Agency Administrator or Executive, resource advisors, and financial arrangements and procedures
- Map/Sketch of the incident
- Incident Action Plan
- Site safety plans
- Evacuation plans
- Other documents

Incident Briefing

The Incident Briefing (ICS Form 201) is the form that is commonly used for the incident briefing. It should be familiar to all who have had ICS training, especially trained IMTs. It is a common form, so if Incident Commanders are coming together to work in Unified Command, they should all recognize it and know how to use it.

During the initial response, the first Incident Commander normally completes the Incident Briefing form. This form and a specific briefing are provided by the initial response Incident Commander to the incoming Incident Commander or Unified Incident Commands if Unified Command is being implemented.

In some cases, the information contained in the Incident Briefing form may only be verbally supplied. Keep in mind that the initial Incident Commander may not be experienced in using the Incident Briefing form but may certainly have the information needed. Good note-taking and questioning by responding ICS organizational members are imperative.

The Incident Briefing form:

- Provides staff with information about the incident situation (to include complexity) and the resources allocated to the incident. This should include objectives, tactics, organization, facilities, communications, and notifications completed.
- Serves as a permanent record of the initial response to the incident.

- Can be used for transfer of command.

Incident Briefing Participants

The facilitator for this Incident Briefing is the current Incident Commander or possibly the incoming Planning Section Chief. The attendees include the incoming Incident Commander and Command and General Staff, as available. Depending on your position within the ICS organization, you may not be a participant in this meeting.

Transfer of Command

Transfer of command is the process of moving the responsibility of incident command from one Incident Command/Unified Command to another. It can be Incident Command to Unified Command or Unified Command to Unified Command. It may be from an ad hoc local Incident Command to an Incident Management Team brought in from outside the jurisdiction to manage the incident. This may also be done to relieve the initial Incident Commander due to many factors, including:

- Lack of experience in this situation
- Formal SOP/SOGs for the agency
- Expertise needed in an operational role
- Relief due to fatigue or other factors

Keep in mind that transfer of command does not always occur. When an Incident Management Team is brought in to support an incident, the IMT does not always assume command. For some incidents, the existing Incident Command/Unified Command remains in place, and the IMT resources are integrated into the existing incident command structure to augment or support (work for) the local Incident Commander or Unified Command.

Transfer of Command Steps

Incoming Incident Commander (Assuming)

1. Assess the situation with the current Incident Commander
2. Receive briefing using the Incident Briefing (ICS Form 201)
3. Determine the appropriate time for the transfer of command
4. Notify others of change in command
5. Reassign or demobilize the current Incident Commander

Outgoing Incident Commander (Transferring)

1. Assess the situation with the incoming Incident Commander
2. Deliver briefing from the Incident Briefing (ICS Form 201)
3. Determine the appropriate time for the transfer of command
4. Notify others of change in command
5. Accept new assignments or demobilize

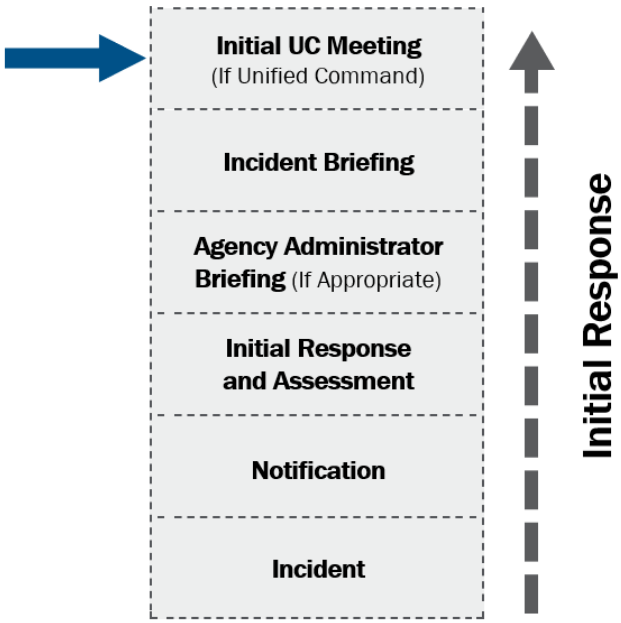
Transfer of Command Briefing

The briefing of the receiving Incident Commander will contain the following information that will be recorded on the Incident Briefing (ICS Form 201):

- Current situation, including objectives, tactics, and organization
- Resources available and status, including facilities, communications, and notifications completed
- Particular areas of concern (political, community interest, etc.). Including a discussion of complexities associated with the incident
- Logistical Support needed or retained
- Turnover of appropriate incident documentation
- Future outlook

Initial Unified Command Meeting

Figure 37: Initial Response: Initial Unified Command Meeting (If Unified Command)



Purpose

The Unified Command Meeting occurs in the Operational Planning Cycle (after the Incident Briefing and before developing the incident objectives). This step is only required for Unified Command situations. Remember back to your Unified Command training how important this meeting is. Members of the UC must make time for it and do it right. Doing this correctly the first time will be critical in the following hours.

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. This is a closed meeting to work out the details of the unified organization, shared facilities, and other Unified Command requirements.

An important aspect of planning under Unified Command is the need for all jurisdictional or functional agency members of the Unified Command to participate in a command meeting early in the incident response.

The unified command meeting provides the responsible Agency Administrators with an opportunity to discuss and concur on critical issues prior to joint incident planning. Requirements for the Initial Unified Command meeting include:

- Prior to the meeting, the members of the Unified Command should have reviewed the purposes and agenda items and be prepared to discuss them.
- The command meeting should only include the members of the Unified Command. Selected staff may be required to brief key information to the Unified Command in this meeting.
- The meeting should be brief, and all-important points and Unified Command decisions should be documented.
- The results of this meeting will guide the overall response effort.

Some examples of decisions that will be made at the Unified Commander's Meeting include:

- Incident name
- Organizations/agencies that will be represented in Unified Command
- Appoint Operations Section Chief and Deputy(s) as necessary
- Command and General Staff composition
- Staffing levels for the IMT (unit level and support)
- Support facilities and locations (ICP, Base, JIC, etc.)
- Operational period and hours of operation
- Critical information reporting thresholds
- Offsite reporting process and timing, e.g., Incident Status Summary (ICS-209), situation reports, Agency Administrator/Agency Executive briefings, etc.
- Media information flow and authorizations
- Resource ordering, cost-sharing, and cost accounting processes

Participants/Attendees at the Initial UC Meeting

The initial UC meeting should be attended by all members of the Unified Command. Other staff that may be needed to support this meeting include the Documentation Unit Leader as the recorder and the Planning Section Chief as the facilitator. Note that there is a limited number of participants. Depending on your position within the ICS organization, you may not be a participant in this meeting.

Sample Initial Unified Command Meeting Agenda

- Statement of specific jurisdictional/agency goals, based on the overarching response priorities.
- Presentation of jurisdictional limitations, concerns, and restrictions.
- Establishment of an agreement on acceptable priorities.
- Discussion of each organization's objectives (note that final objectives are developed when the Incident Command/Unified Command Develops Incident Objectives step).
- Agreement on the basic organizational structure for the Unified Command (note that the Operations Section normally defines their section structure in the Tactics meeting based on objectives, requirements, and resources).
- Designation of the best qualified and acceptable Operations Section Chief.
- Agreement on General Staff personnel designations.
- Agreement on planning, logistical, and finance agreements and procedures.
- Agreement on resource ordering process to be followed.
- Agreement on cost-sharing procedures.
- Agreement on informational matters.

Designation of one of the members of the Unified Command to act as the Unified Command spokesperson.

Establishing Incident Priorities

As part of their framework for managing the incident, the Incident Commander or Unified Command must define overall priorities for the incident response. Priorities, leader's intent, objectives, strategies, and tactics define the direction that the ICS organization will take to respond to the incident. Together these will define what resources are needed to manage the incident and what ICS organizational elements (staff) are needed to effectively manage those resources and accomplish the objectives.

According to the National Response Framework (NRF), the highest priorities of response are to:

- Save lives
- Protect property and the environment
- Stabilize the incident
- Meet human needs by stabilizing Community Lifelines
- Prepare for recovery considerations

The overall NRF response priorities guide is similar, but not identical to, the priorities established by the Incident Commander/Unified Command during an incident. For example, saving lives is a priority for response; but in an incident, the safety of responders is commonly prioritized above saving the lives of those affected by the incident. Life safety is an overall priority, but in this example, the Unified Command may clarify that they do not

want to unnecessarily jeopardize the life safety of the responders in attempts to rescue members of the public impacted by the incident.

Another example of an incident priority would be, "The rail car is spilling hazardous materials. It is a priority for this incident that we try to prevent those hazardous materials from entering the reservoir, which is a source of the jurisdiction's drinking water." Priorities can also include items such as "Gain increased situational awareness of community impacts by 1800 hrs."

It is also important to understand that priorities are not mutually exclusive. You do not have to complete one priority before you can begin another. It is normally possible to support multiple priorities simultaneously. Priorities lead to objectives and should be aligned to avoid confusion and also to give staff an overall high-level understanding of the "Big Picture." (USFA NFA, 2016)

Defining the Length of the Operational Period

The initial determination of the operational period may change later in the planning cycle based on the development of the incident, even though the initial determination is made in the Unified Command meeting.

The NIMS definition of an "operational period" is the time (e.g., 0700 – 1900 hours) scheduled for executing a given set of operational actions (e.g., tactical, field operations) as specified in the incident action plan. NIMS/ICS utilizes the term operational period as the effective time for the Incident Action Plan and the activities contained within.

The NWCG defines the operational period as the period of time scheduled for executing a given set of tactical actions as specified in the Incident Action Plan.

As a result, all ICS incident action planning is based on identifying the expected tasks to be completed over a specific time period called the operational period. The specific length of time of the operational period varies based on a list of factors. There are implications to these decisions that the Incident Commander should consider. These factors are:

- Safety conditions – Safety of responders, victims, and others is always the first priority of any response.
- How dynamic is the incident, or how quickly are conditions changing? If the Operations Section Chief's tactical plan is only valid for a limited period of time due to changing conditions (e.g., exponential growth, weather, values at risk, etc.), then a 12-hour operational period may be appropriate. If the conditions are stable enough for a longer tactical plan, then a 24-hour operational plan may be appropriate. Remember that resources can be replaced, and shift changes can occur within the 24-hour operational period, e.g., Assignment List (ICS-204) for A.M. resources and Assignment List (ICS-204) for new P.M. resources.

- Condition of resources – Planning must be done far enough in advance to ensure that additional resources needed for the next operational period are available.
- The length of time necessary or available to achieve the tactical assignments.
- Availability of fresh resources.
- Future involvement of additional jurisdictions or agencies.
- Environmental conditions – Factors such as the amount of daylight remaining, and weather and wind conditions can affect decisions about the length of the operational period.

The Incident Commander will determine the length of the operational period with input from staff. In some cases, the operational period length may change from day to day based on operational and incident needs.

The length of an operational period depends on the nature and complexity of the incident. Common lengths of operational periods are:

- 12, or 24 hours depending on the nature and complexity of the incident and the working conditions such as weather, safety, and anticipated fatigue.
- The final decision on the length of an operational period rests with the Incident Commander and is dependent upon the needs and risks of the incident.
- Multiple days for relatively stable situations and recovery actions such as debris removal.

Operational Shifts

Operational periods should not be confused with shift hours. A shift is the assigned work period – it relates to when an individual starts and ends their work period in an incident. Time off shift is used for rest and refitting in preparation for a future work period. The use of shifts to define the active work periods of incident personnel is generally based on safety or contractual issues.

In some cases, the end of the operational period may also align with a shift change. You may have one or more shift changes or crew rotations within an operational period if needed. For example, in an incident with a 24-hour operational period, there may be two or three shifts. In an incident with very short operational periods, a single shift may be engaged in more than one operational period. An example of this is a Hazmat incident with a 4-hour operational period in which one shift may work through two operational periods. Another example is a high-rise structure fire involving overly strenuous hauling of hose and stair climbing.

Operational Rhythm and Operational Tempo (these are not NIMS terms)

You may hear the terms “battle rhythm” or “operational rhythm” in relation to operations. Some organizations have adopted these terms and, in some cases, may use them interchangeably with operational periods. These are not the same thing. Operational Rhythm

is a term with a much less specific connotation than the term operational period. This broader connotation includes activities such as aligning the schedules for the field operational period by the IMT, EOC activities (e.g., meetings, calls, reports, etc.), and State EOC activities (e.g., meetings, calls, reports, etc.) to ensure proper coordination.

Battle rhythm is the military term for the maintenance of an ordered routine. The U.S. Department of Defense defines the term as the deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations. Operational rhythm is a term some ICS organizations have adopted to refer to the same concept.

An Operational Rhythm refers to the operational schedule and is about ensuring that certain vital activities are performed consistently to a high degree of excellence both across and within the incident. The key aim is to drive efficiency, effectiveness, and, therefore, productivity. Operational rhythm is not the same as the operational period planning cycle – it supports the planning cycle.

An example of an ICS organizational activity that is not defined in the Operational Period Planning Cycle (Planning P) but should be accomplished on a defined timeline within each operational period is updating the Common Operating Picture displays in the Incident Command Post. The Planning P does not address this activity, but it is something that should occur regularly during the operational period. An operational rhythm would define when the incident command wants key activities such as this to occur.

The Operational Rhythm should be established as soon as possible to support the Command and General Staff decision-making process. (DTD Joint Staff J7, 2019)

The Planning Section Chief normally will develop this based on guidance from the Incident Commander/Unified Command.

The operational rhythm should align with the operational period planning cycle meeting schedule. The defined deadlines for informational updates ensure that the information and knowledge relevant to managing the incident is available when needed for each incident action planning process meeting and briefing. Following synchronized timelines keeps information consistently flowing through the All-Hazards Planning Cycle. An Incident Action Plan (IAP) is developed and produced for the next operational period, and the planning cycle begins again. Adhering to the established operational rhythm keeps the ICS organization on track and successful in accomplishing the incident objectives.

“Operational tempo” is another time/schedule-related term that you may hear. The NWCG defines operational tempo as the speed and intensity of our actions relative to the speed and intensity of unfolding events in the operational environment. Within this context, fire leaders plan, prepare, and execute operations proactively, rather than continuously being forced to react to the environment. Simply put, it is the schedule of how your team is going to stay in sync and follow a commonly agreed-upon schedule of meetings and operations.

The term operational rhythm should not be confused with or substituted for the operational period planning cycle. ICS organizations should use common language that has a defined, commonly understood meaning. It is recommended that the ICS organization use the term operational period when referring to the defined period of time to accomplish a set of activities defined in the IAP.

Chapter 7: Ongoing Response

Incident Action Planning Process – Ongoing Operations

The leg of the "P" activities detailed in the previous chapter are those activities that incident personnel perform only one time in an incident. Once they are accomplished, incident management shifts into a cycle of planning and operations, informed by ongoing situational awareness and repeated each operational period.

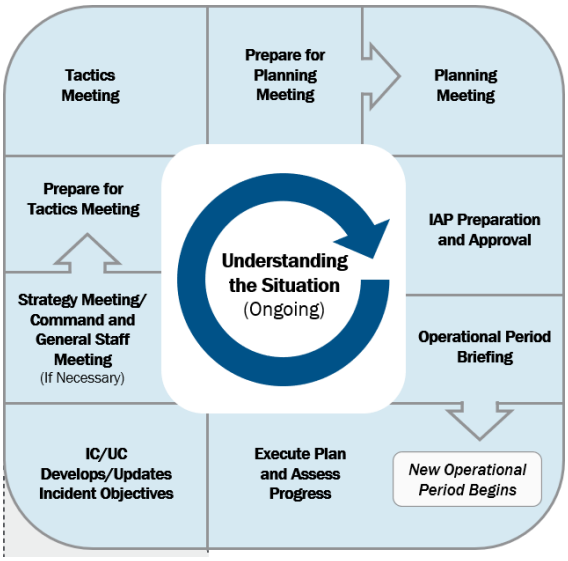
The following are brief descriptions of the meetings and briefings that are repeated each operational cycle until the conclusion of the incident or event.

- Objectives Development/Update: The Incident Command/Unified Command establishes the incident objectives for the initial operational period. After the initial operational period, the Incident Command/Unified Command reviews the incident objectives and may validate them, modify them, or develop new objectives.
- Initial Strategy Meeting/Command and General Staff Meeting: After developing or revising the incident objectives, the Incident Command/Unified Command typically meets with the Command and General Staff, and sometimes others, to discuss the incident objectives and provide direction.
- Preparing for the Tactics Meeting: One of the first steps to preparing for the meeting is to evaluate the incident and the effectiveness of current tactics before developing new ones. The Operations Section Chief will obtain information and recommendations from field supervisors (such as Division/Group Supervisors or Branch Directors if the positions are established) to help determine tactics for the next operational period. 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: In the Tactics Meeting, key players review the proposed tactics developed by the Operations Section and conduct planning for resource assignments. The Operations Section Chief leads the Tactics Meeting, and key participants include the Logistics Section Chief, Safety Officer, a Resources Unit Leader, and other invitees.
- Preparing for the Planning Meeting: Following the Tactics Meeting, staff collaborates to identify support needs and assign specific resources to accomplish the 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. At the end of the Planning Meeting, Command and General Staff confirm that they can support the plan.

- Incident Action Plan (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.
- Operational Period Briefing: Each operational period starts with an operational period briefing. Incident supervisory and tactical personnel receive the IAP during the briefing. Members of the Command and General Staff present the incident objectives, review the current situation, and share information related to communications or safety. During the briefing, Operations will go over tactical work assignments for resources.
- Following the operational period briefing, supervisors brief their assigned personnel on their respective assignments.

At this point, a new operational period begins. The next step is to Execute Plan and Assess Progress, after which the cycle begins again.

Figure 38: Operational Period Planning Cycle – the Cycle of Ongoing Operations



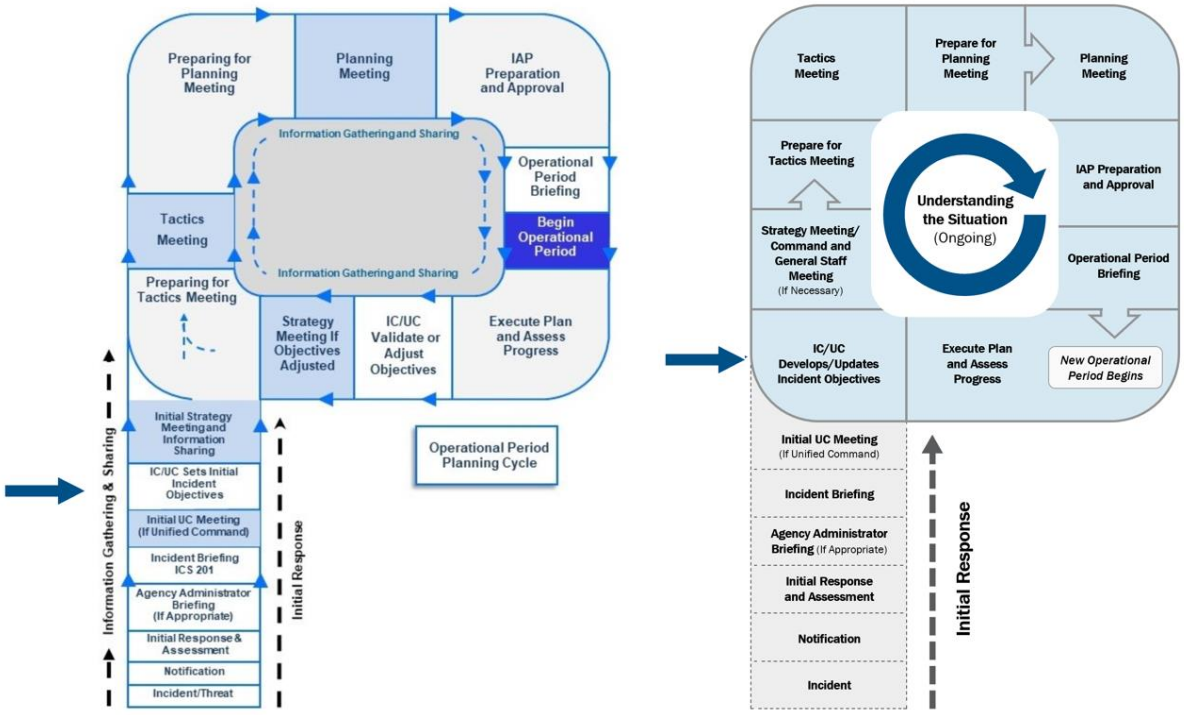
Incident Command/Unified Command: Develop/Update Incident Objectives

Purpose

Regardless of the size or complexity of the incident, one of the most important things the Incident Command or members of the Unified Command do is to establish a common set of incident objectives. This must be done at this point for the rest of the Command and Staff members to carry out the mission. Incident objectives may change as new information comes in, but the Incident Command/Unified Command needs to do this now to keep up the momentum and encourage everyone to be working towards the same end.

During the initial Incident Command/Unified Command meeting, the members of the Incident Command/Unified Command identify their agency's policies, limitations, management objectives, etc. This information must be blended into one set of unified incident objectives. In a single command, this is done by the one Incident Command.

Figure 39: Comparison of All-Hazards and NIMS 2017 Planning P



Variations in the Planning P

The All-Hazards version of the Planning P places the development of incident objectives in two places on the Planning P: once during the initial response and again after ongoing operations are initiated. The NIMS Planning P only depicts this as one action that happens each operational cycle.

It is important to note that the sequence of events is the same, but the All-Hazards Planning P places the initial Objectives development in the leg of the P (Initial Response) to convey a very specific meaning. In the All-Hazards Planning P, the Incident Command/Unified Command sets the Initial Incident Objectives step and places it in the Initial Response actions because this is an action that is only done once in an incident.

Some activities occur in setting the initial objectives during the initial response that do not re-occur when objectives are validated and adjusted during each subsequent operational cycle. The separate meeting in the ongoing operations section of the All-Hazards Planning P labeled *Incident Command/Unified Command Validate or adjust objectives* depicts an activity that occurs every operational period. This highlights that the Incident

Command/Unified Command takes actions in the initial response that are not taken in the subsequent operational periods. Examples of these actions include establishing the initial operational schedule for the first operational period and establishing ground rules under which the ICS organization will function.

Whatever version of the Planning P is used by your organization, it is important to understand that there are aspects of the Incident Command/Unified Command development of incident objectives that will occur only in the initial response and will not normally need to be repeated in subsequent operational periods.

Participants

The Command and General Staff usually contribute to the development of incident objectives. However, the Incident Command or Unified Command is still responsible for the incident objectives.

Although the Operational Period Planning Cycle does not specify the exact time the initial strategy is selected, it is often done during this meeting.

The designated Operations Section Chief should participate in the selection of the strategy.

The incident objectives are assessed by the Incident Command/Unified Command at the start of the Operational Period, before the tactics meeting, and updated as needed. Here are some questions to ask when assessing objectives:

- Is the incident stable, or is it increasing in size and complexity?
- What are the current incident objectives, strategies, and tactics?
- Are there any safety issues?
- Are the objectives effective? Is a change of course needed?
- How long will it be until the objectives are completed?
- What is the current status of resources? Are resources in good condition? Are there sufficient resources?

When immediate action is required, changes may be implemented prior to the issuance of the next written IAP.

Incident Objectives

Incident objectives are derived from problems and priorities. They are achieved through strategies and tactics:

- **Incident objectives** state what is to be accomplished in the operational period.
    - The current incident objectives may be found on the Incident Briefing (ICS Form 201) or Incident Objectives (ICS Form 202).
    - The Incident Commander/Unified Command establishes the incident objectives and may provide broad strategic direction.

- **Strategies** establish the general plan or direction for accomplishing the incident objectives.
  - The Incident Commander has created and briefed the incident objectives.
  - The Operations Section Chief translates the objectives and strategies into tactics.
- **Tactics** specify how the strategies will be executed.

"SMART" Objectives

Incident objectives should have the following SMART characteristics:

- **Specific.** The wording must be precise and unambiguous in describing the objective.
- **Measurable.** The design and statement of objectives should make it possible to conduct a final accounting as to whether objectives were achieved.
- **Action-Oriented.** The objective must have an action verb that describes the expected accomplishments.
- **Realistic.** Objectives must be achievable with the resources that the agency (and assisting agencies) can allocate to the incident, even though it may take several Operational Periods to accomplish them.
- **Time Sensitive.** The timeframe should be specified (if applicable – in some cases, an objective may not include a specific time to complete because it is not time-bound).

How to Write a Good Objective

Writing an objective that is both specific and measurable can be an art. Many times, draft objectives can be established in advance for common types of incidents or threats. This can provide a 90%+ solution that needs to be tweaked during the actual response. This helps reduce some of the stress/pressure during the Objectives Meeting and results in a more professional product. Perhaps the best way to convey this art is to teach by example, but some basic rules may be helpful.

1. State the objective. Begin the objective by stating what has to be accomplished - the goal. "Prevent fire from reaching Sunnybrook Lake subdivision" is a good start. Writing "Dig a fire line between the Sunnybrook Lake subdivision and the fire" is not advisable because this second statement deals with how the objective is going to be accomplished. How a statement like this fits into the objective will be covered in Rule #4.
2. Give details. Provide enough detail to make the objective meaningful. "Control fire within 24 hours of the first attack" is a good start. "Put the fire out" is not ok.
3. Can results be measured when the objective is met? When the fire is out, "yes" or "no" should answer the question, "Was the objective accomplished? This is what we mean by measurability. "Preserve historic lodge structures in the east end of the park" is measurable. In other words, one can observe historic lodge structures after the fire and determine whether they were preserved or not. "Minimize damage to historic structures"

is not measurable. For one thing, people may differ on what is meant by minimal damage. At the very least, one should be able to measure the outcome against the objective in a meaningful way: "All but one of the lodge buildings remain undamaged." "Burned acreage exceeded the objective by 10%." "90% of the spotted owl nesting territory was preserved."

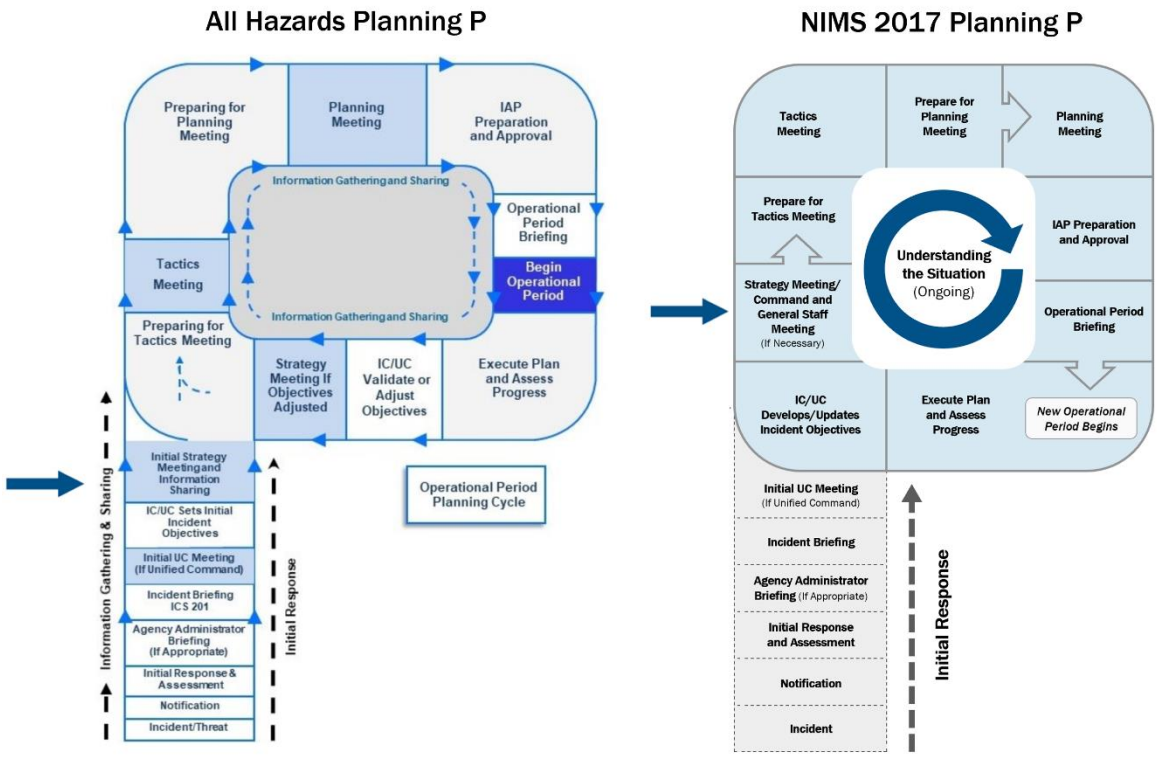
Leading and Lagging Indicators. A leading indicator tells you in advance that you are progressing toward meeting an objective. A lagging indicator tells you at the end if you have or have not met the objective. For example, "preserve historic lodge structures at the east end of the park" is a good measure, but it is a lagging indicator – at the end of the fire, they are either preserved or not preserved. A leading indicator would be something that indicated if you were going in the right direction. For example, "prevent any fire from entering the east end of the park beyond fire-break 17E to preserve historic structures in the east end of the park." If the fire crosses the firebreak, the historic structures aren't necessarily lost, but you have created an indicator that allows you to see that an objective is in danger of not being met while allowing space for additional actions to be taken to accomplish the objective. When possible, set objectives that are measurable using leading indicators. A final note: sometimes leading indicators are built into the Incident Commander/Unified Command's Essential Elements of Information (EEI) as "decision points" or "trigger points" to let them know something is threatening an objective, and additional actions must be taken to ensure that the objective is accomplished.

4. How is it going to be done? Where possible, include guidelines for how the objective is to be accomplished. "Keep firefighter injuries and accidents to zero" is an incomplete objective, but if you add the enabling phrase "….by reducing time on the line and in the air," the objective takes on additional meaning in the context of the current fire. Our example in Rule #1 would now read, "Prevent fire from reaching Sunnybrook Lake subdivision by constructing a fire line between the subdivision and the fire." This information is important because it gives the chance to evaluate the fire response directly against the objective. For example, let's say the objective is "Preserve Pre-Columbian ruins on the south end of the ridge." Before the Incident Management team is deployed, the wind shifts and the fire moves in an entirely different direction and stops threatening the ruins. The objective is accomplished. To say that the selected strategy was effective in accomplishing the objective may be misleading, however. "Preserve Pre-Columbian ruins on the south end of the ridge by directly attacking fire at its southern extremity" allows us to determine that the happy ending, in this case, was not due to the selection of a particular strategy.
5. Is the objective reasonable? Some objectives are worthy in theory but cannot be met in practice. For example, the objective "keep total loss and suppression costs under $1,000 by using local volunteers and free resources" sounds like a great idea, but it is

not reasonable because there is no chance of this being accomplished while responding to a 500-acre fire.

Strategy/Command and General Staff Meeting

Figure 40: Planning P Variations – Initial Strategy Meeting/Command and General Staff Meeting



Variations in the Planning P

Note that in the NIMS 2017 Planning P, we are already in the second activity of Ongoing Operations, while in the All-Hazards Planning P, we are in the final step of Initial Response. Again, the sequence is the same, but the placement is different.

The All Hazards Planning P does not refer to this as the Command and General Staff Meeting. It is called the Initial Strategy Meeting. In the All-Hazards community, the Command and General Staff Meeting are not in the Planning P because it is a meeting that occurs at different times, as needed--it is not a strategy meeting.

The USCG Planning P calls the Strategy Meeting the Command and General Staff Meeting; however, it has the same purpose – to develop strategies.

Purpose

After developing or revising the incident objectives, the Incident Commander/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.

Note that the NIMS 2017 Planning states that this meeting is held "If Necessary." This meeting may not need to happen if the Agency Administrator's direction remains the same from one operational period to the next or if incident objectives do not change. If the ICS organization is entering a new operational cycle, the current approach is working, and there are no significant changes to the incident that would require new or adjusted objectives, there is no need to hold the meeting. This will be a decision by the Incident Commander or Unified Command. The meeting must occur in the initial response to set objectives. The meeting will most often happen again in each of the first couple of operational periods when the incident may be most unstable and require significant adjustments in strategy, tactics, and objectives. It may become less required in later operational periods when the incident is stabilized.

Participants

This is a short, private meeting between the Incident Command/Unified Command and the Command and General Staff. This may not take place in some low-complexity incidents because there are few supervisors. In those cases, the Incident Commander/Unified Command may be the only participant in objectives development. However, for more complex incidents, it is imperative for an ICS organization to do this step to make sure everyone is on board with the incident objectives and sets the stage for a successful first IAP.

The ICS organization may be asked to start managing the incident now as well as begin the planning process for the next operational period. This happens when initial responders are overwhelmed and need relief immediately.

The initial Strategy Meeting, which is held the first time through the planning cycle, is particularly important because it allows the Incident Command/Unified Command and Command and General Staff members to share information and jointly determine the initial approach to the response.

The goal of the Strategy/Command and General Staff Meeting is to:

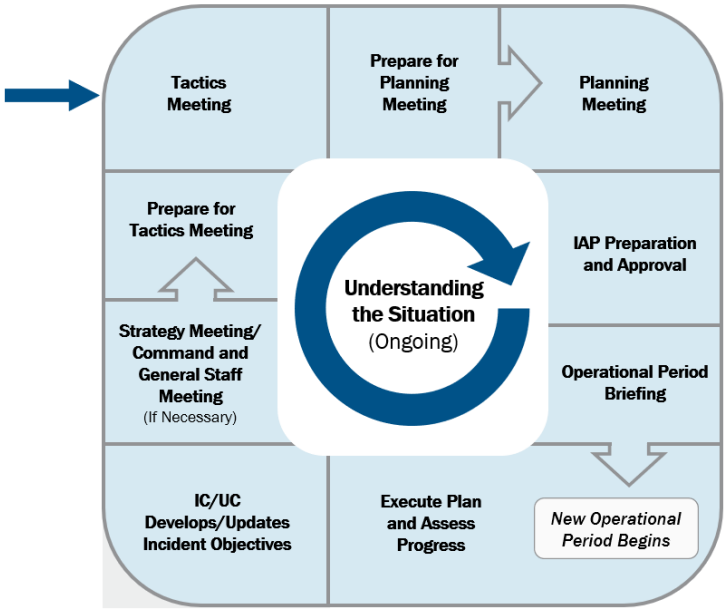
- Incident Command/Unified Command share leader's intent, priorities, incident objectives, and solicit input
- Announce the Operational Period and meeting schedule
- Discuss key decisions and concerns
- Share information

The Operations Section Chief will then develop the initial strategies to meet the Incident Command/Unified Command's incident objectives and ensure they:

- Are within acceptable safety norms
- Make good sense (effective, feasible, practical, and suitable)
- Are cost-effective
- Are consistent with sound environmental practices
- Attempt to meet external influences, e.g., political, social, economic, etc.

Tactics Meeting

Figure 41: Operational Period Planning Cycle – Tactics Meeting



Purpose

The purpose of the Tactics Meeting is to review the proposed strategy and tactics developed by the Operations Section. This includes:

- Determining the tactics for the selected strategy or strategies that will be accomplished to achieve the incident objectives.
- Assigning resources to implement the tactics.
- Identifying methods for monitoring tactics and resources to determine if adjustments are required (e.g., different tactics, different resources, or new strategy).

The Tactics Meeting is rather informal. It typically occurs 1 to 4 hours prior to the Planning Meeting. Once the ICS organization has become familiar with the dynamics of the incident and challenges with resources, ordering, etc., the time needed for the Tactics meeting typically decreases.

The Operational Planning Worksheet (ICS Form 215) and Incident Action Plan Safety Analysis (ICS Form 215A) are products (outputs) of the Tactics Meeting.

Preparing for the Tactics Meeting

Once the incident objectives are 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. The Planning Section will assist in the form of a Resources Unit Leader (if available), who will provide the most current input on what resources have been ordered and expected in time for the operational period but have not yet checked in. If a Resources Unit Leader has not been appointed, then the Plans Section Chief will generally fill this role.

Note that this is a distinct step in the planning cycle "Preparing for the Tactics Meeting." It is not a meeting; it is a period of time in which key preparation activities occur that will enable final decisions to be made during the Tactics Meeting. During this time, the Operations Section Chief will solicit input from field supervisors/directors (Branch Directors, Division, Group Supervisors, etc.) on the status of the incident in their area, progress on current tactics, recommendations, and resource requirements for the next operational period prior to the formal meeting.

Three common approaches to preparing for the Tactics Meeting:

1. Operations Section Chief has a draft paper copy of the Operational Planning Worksheet (ICS Form 215), filled out before the meeting, allowing the Resources Unit Leader to complete the wall size Operational Planning Worksheet before the Tactics Meeting. An advantage to this method is that less time is spent during the meeting since the bulk of the work is completed prior. Also, the Operational Planning Worksheet is in the Resources Unit Leader's handwriting; this avoids issues arising later if the Resources Unit Leader cannot decipher someone else's handwriting on the Operational Planning Worksheet.
2. Operations Section Chief begins the process during the meeting. The Operations Section Chief dictates while the Resources Unit Leader completes the form. (Least desirable since this can take a lot of time.)
3. A less common approach is for the Operations Section Chief to describe the tactical plan in broad terms at the Tactics Meeting to the attendees. It is then the responsibility of the Operations Section Chief to deliver the completed paper copy of the Operational Planning Worksheet one hour before the Planning Meeting allowing the Resources Unit Leader time to transfer the plan to the wall-sized Operational Planning Worksheet. The LSC/SOFR will have little time to adjust if there are flaws.

After reviewing the Operational Planning Worksheet for potential risks and discussing with the Operations Section Chief, the Safety Officer determines mitigation measures and documents both on the Incident Action Plan Safety Analysis (ICS Form 215A).

The Operational Planning Worksheet is designed to document the results of the Tactics Meeting. The Operational Planning Worksheet displays:

1. Branches (if applicable)
2. Division by geography
3. Group by function
4. Work assignments
5. Quantity, kind, and type of resource plus availability (Requested, Have, or Needed)
6. Reporting location for resources
7. Requested arrival time of resources

This worksheet should be completed at least one to two hours before the Planning Meeting. Keep in mind that during large incidents, there may be several Operational Planning Worksheets (ICS 215s) in use at the same time to manage resources. Typically, you might have them separated by group, division, or branch.

Some ICS organizations use a computer and projector to display and complete the Operational Planning Worksheet. The Resources Unit Leader operates the computer.

Developing Tactical Direction

Tactical direction is developed based on the incident objectives. It describes what must be accomplished within the selected strategy or strategies to achieve the incident objectives. Tactical direction is the responsibility of the Operations Section Chief. If an Operations Section Chief has not been assigned, then the Incident Command/Unified Command takes responsibility for developing tactics.

Gathering input is particularly important when the incident involves personnel from multiple disciplines. Jointly developed tactics can ensure understanding and enhance commitment. To accomplish this, the Operations Section Chief gathers input from the Branch Directors and Division and/or Group Supervisors.

Tactical direction consists of the following steps:

- **Establish Tactics.** Determine the tactics needed to implement the selected strategy. Typically, tactics are to be accomplished within an Operational Period. During more complex incidents, a tactical direction should be specified in terms of achievements that can be realistically accomplished within the timeframe currently being planned.
- **Assign Resources.** Determine and assign the kind and type of resources appropriate for the selected tactics. Resource assignments will consist of the kind, type, and number of resources available and needed to achieve the tactical operations desired for the operational period.
- **Monitor Performance.** Performance monitoring will determine if the tactics and resources selected for the various strategies are both valid and adequate. Note that the monitoring of performance is ongoing and does not occur only in this step of the

planning process. The key point for the Tactics Meeting is to identify how performance will be monitored.

When determining tactical operations, consider the following personnel and logistical support factors:

- If the required tactical resources are not available, then an adjustment should be made to the tactics and operations planned for the operational period.
- The lack of logistical support can mean the difference between success and failure. Lack of available resources could require a reassessment of tactics and perhaps the overall strategy.

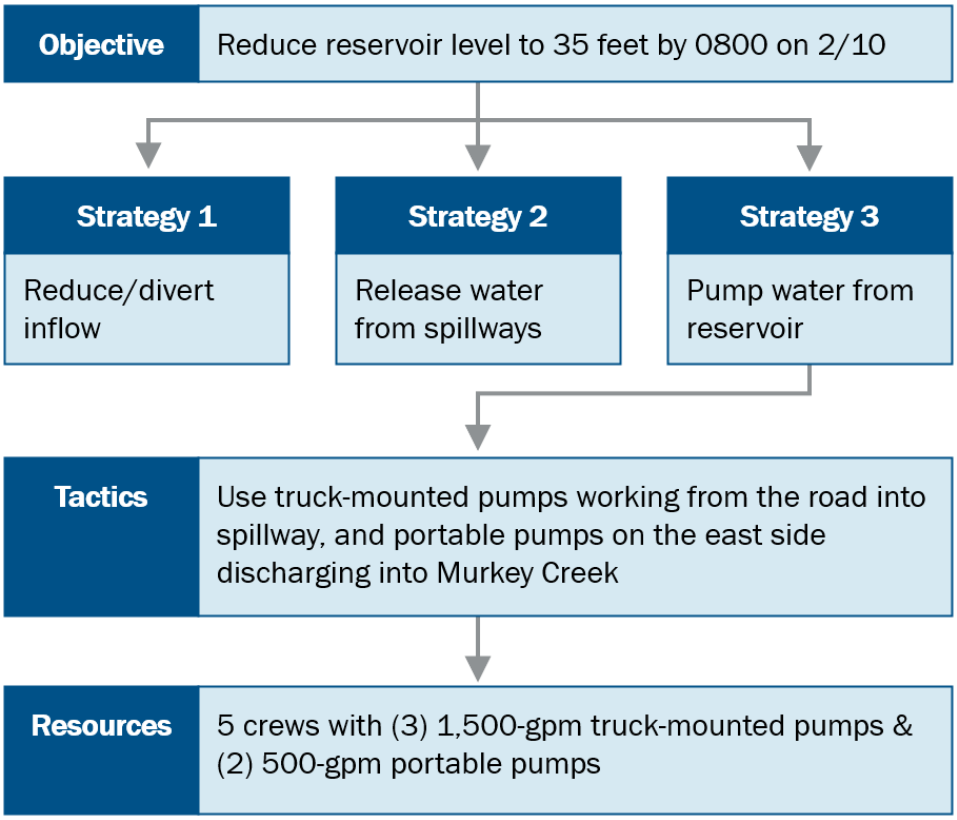
It is very important that tactical resource availability and other needed support are determined before investing time on strategies and tactical operations that realistically cannot be achieved.

Tactical planning is dependent on resource availability and may affect the accomplishment of objectives.

Sample Objective, Strategies, and Tactics

The following is an example of the relationship between objectives, strategies, and tactics and how they migrate from a high level to a more actionable level of response.

Figure 42: Sample Objective, Strategies, and Tactics



Technique for determining the strategies and tactics based on a sample objective:

- The **objective** is: Reduce the reservoir level to 35 feet by 0800 on 2/10.
- Three possible **strategies** are identified, and one is selected: Pump water from the reservoir.
- The **tactics** for the selected strategy are to use truck-mounted pumps working from the road into the spillway and portable pumps on the east side discharging into Murkey Creek.

Once the tactics have been selected, the next step is to determine what and how many resources will be needed to accomplish the tactics. Safety must also be reviewed to determine hazards, evaluate risks and assign controls to reduce risk.

Cost-Benefit Analysis in Tactics and Resource Selection

The Cost Unit within the Finance/Administration Section provides all cost analysis, including cost-benefit analysis, for the organization. For example, the use of National Guard resources for transportation may be more expensive than contracting locally for the same resource.

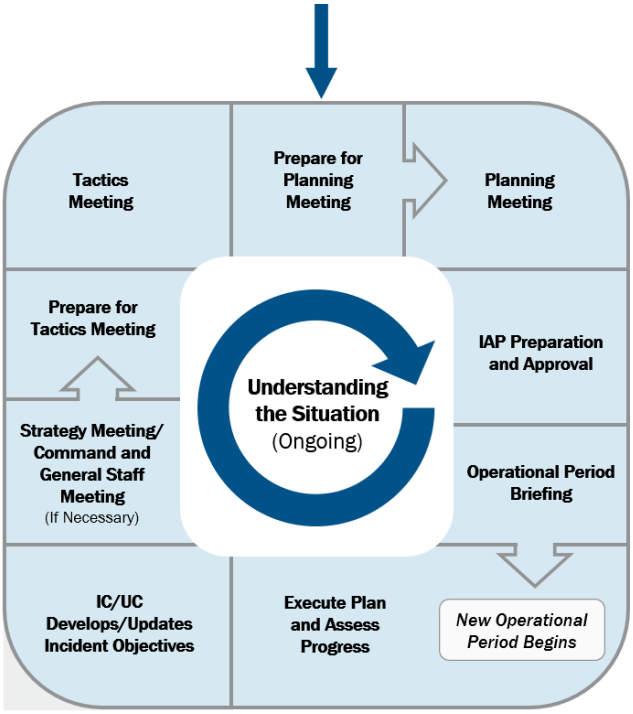
Some cost-benefit considerations include:

- What alternatives are available to accomplish the selected tactic?
- What are the estimated costs of these alternatives?
- What are the benefits of each alternative?
- What are the safety factors of these alternatives?
- What are the time variables of these alternatives?
- Which of the alternatives has the highest cost-benefit ratio? (A ratio of 1:1 would indicate the cost of the alternative equals the benefits derived from using that alternative.)

An example might be to compare using a helicopter to put out a grass fire when a brush truck would accomplish the same task. Both are effective, but one has a much higher inherent risk factor as well as a higher cost.

Preparing for the Planning Meeting

Figure 43: Operational Period Planning Cycle – Preparing for the Planning Meeting



Purpose

The next step in the incident action planning process is to prepare for the Planning Meeting. Following the Tactics Meeting, the Planning Section coordinates preparations for the Planning Meeting. These preparations include the following activities:

- Analyze the Operational Planning Worksheet (ICS Form 215) (prepared by the Operations Section Chief) developed in the Tactics Meeting
- Ensure the proposed strategies and tactics meet the Incident Commander/Unified Command's operational objectives
- Finalize an Incident Action Plan Safety Analysis (ICS Form 215A) (prepared by the Safety Officer) based on the information in the Operational Planning Worksheet (ICS Form 215)
- The Operations Section Chief assesses current operations effectiveness and resource efficiency
- Gather information to support incident management decisions
- Ensure displays for critical information are ready and updated
- Verify that the resources needed to carry out tactics are accounted for and can meet timeframes defined in the IAP
- "Share" the proposed plan with the Incident Commander and other members of the ICS organization that were not at the Planning Meeting to avoid or minimize conflicts during the actual meeting

Displays that should be prepared for the Planning Meeting should include:

- The meeting agenda
- Incident objectives
- Large versions of the Operational Planning Worksheet (ICS Form 215) and Incident Action Plan Safety Analysis (ICS Form 215A)
- Maps/charts
- The schedule for forms submission and additional meetings
- Any props needed to illustrate the proposed tactical plan

Figure 44: Sample Displays

Contributors/Attendees

This list includes attendees of the planning meeting and how each contributes to the process. Most of these activities require forethought and preparation by the Command and General Staff members before the actual Planning Meeting.

Incident Commander or Unified Command

- Gives direction
- Communicates
- Manages
- Avoids getting unnecessarily involved in the details

Safety Officer

- Identifies incident risks and mitigations
- Completes Incident Action Plan Safety Analysis (ICS Form 215A) developed at the tactics meeting
- Works with the Operations Section Chief on tactical safety issues
- Identifies safety issues associated with incident facilities and nontactical activities, such as transportation and food service

Liaison Officer

- Identifies cooperating and assisting agencies
- Identifies special agency needs
- Determines capabilities of cooperating and assisting agencies
- Determines restrictions on the participation of cooperating and assisting agencies
- Confirms the name and contact location of agency representatives

Public Information Officer

- Assesses general media coverage to date
- Identifies incident-related information issues that need to be explained or corrected with the media
- Determines what Joint Information System (JIS) elements and procedures are in place
- Determines process for development and approval of media releases and visits
- Advises staff on media and social media policies

Operations Section Chief

- Continues to obtain good incident resources and status information
- Communicates current information

- Considers alternate strategies and determines probable tactics
- Calculates resource requirements
- Works with the Safety Officer and Planning Section staff to complete Operational Planning Worksheet (ICS Form 215) and Incident Action Plan Safety Analysis (ICS Form 215A) developed at the tactics meeting

Planning Section Chief

- Prepares incident maps and displays, as necessary
- Develops information for the IAP
- Develops situation status and predictions
- Acquires information and facilitates completion of ICS forms for the IAP

Logistics Section Chief

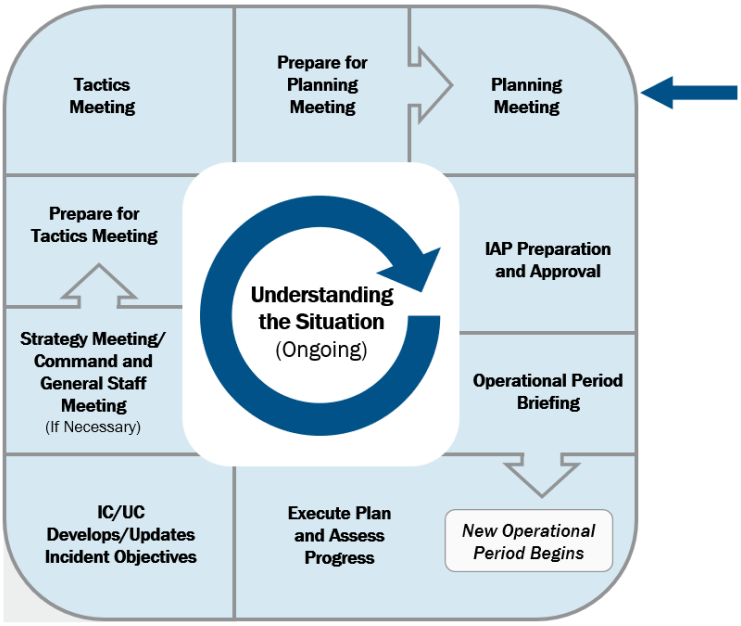
- Determines service and support needs for the incident
- Determines responder medical and rehabilitation needs
- Determines incident communications needs
- Confirms resource ordering process

Finance/Administration Section Chief

- Collects information on rental agreements and contracts
- Determines potential and actual claims
- Calculates incident costs to date
- Develops cost-benefit analyses as requested

The Planning Meeting

Figure 45: Operational Period Planning Cycle – Planning Meeting



Purpose

The purpose of the Planning Meeting is to put the finishing touches on the Operational Planning Worksheet (ICS Form 215), gather support for the Incident Action Plan (IAP) for the next operational period from the Command and General Staff, and gain IAP approval from the Incident Commander/Unified Command.

The Planning Meeting provides the final opportunity for the Command and General Staff, as well as other incident management personnel, agency administrators, and cooperating/assisting agencies and organizations to review and validate the Operational Plan and resource assignments proposed by the Operations Section Chief. At the end of this meeting, the Incident Commander or Unified Command must approve the plan before the development of the formal IAP.

The Operations Section Chief presents the tactical plan using the Operational Planning Worksheet. The Operational Planning Worksheet delineates operations section organization, work assignments, and the amount and kind/type of resources needed to accomplish the plan. It also defines the reporting location and time for resources. The Planning Section's Resources Unit will have to work with the Logistics Section to fulfill these resource requirements.

The Planning Section Chief facilitates the meeting following a fixed agenda to ensure that the meeting is efficient while allowing each organizational element to assess and acknowledge the plan.

At the conclusion of the meeting, the Planning Section Chief indicates when all elements of the plan and support documents must be submitted so the final Incident Action Plan can be collated, reviewed, approved, duplicated, and made ready for the operations briefing.

Participants

- Situation Unit Leader
- Planning Section Chief
- Incident Commander
- Operations Section Chief
- Logistics Section Chief
- Safety Officer
- Finance/Admin Section Chief
- Liaison Officer
- Public Information Officer

Sample Planning Meeting Agenda – Short Version

This sample agenda is included as a short guide to indicate who needs to be in attendance and a suggested order of how those individuals would present their respective information.

- Current Situation - Operations Section Chief
- Incident Objectives - Planning Section Chief
- Weather Forecast - Meteorology Technical Specialist
- Ground Operations - Operations Section Chief
- Safety Plan - Safety Officer
- Air Operations Plan - Air Operations Branch Director
- Information Plan - Public Information Officer

TEAM CONSENSUS

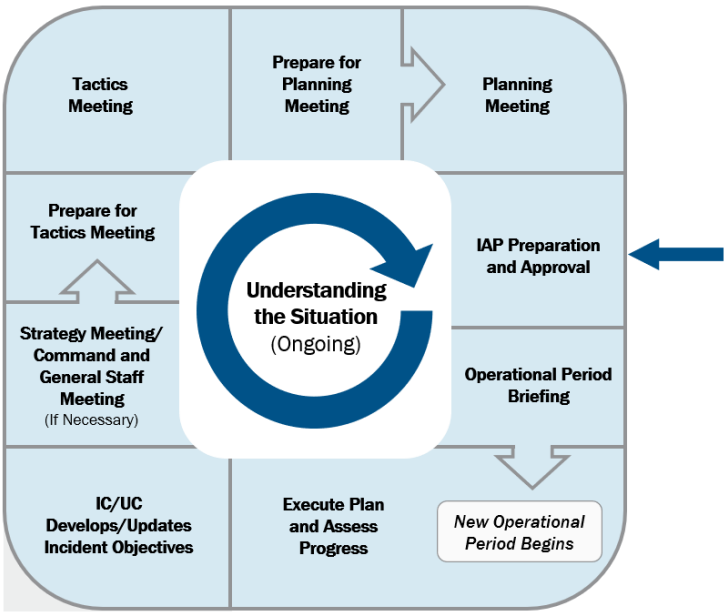
- Logistics Section Chief
- Communications Unit Leader
- Medical Unit Leader
- Finance/Administration Section Chief
- Human Resources Specialist
- Training Specialist
- Cooperating Agencies (Law Enforcement/S.O./Red Cross, etc.)

CONCERNS

- IAP Components Due
- Next Briefing and Planning Meeting
- Closing Comments

IAP Preparation and Approval

Figure 46: Operational Period Planning Cycle – IAP Preparation



Purpose

After the Planning Meeting is held, the following actions are taken to prepare the Incident Action Plan (IAP):

- ICS Staff Sections prepare their components of the IAP and submit them to the Planning Section.
- The Planning Section collates, prepares, and duplicates the IAP document for distribution at the operations briefing. The Planning Section will:
  - Set the deadline for completing IAP attachments.
  - Obtain plan attachments and review them for completeness and approvals.
  - Review the IAP to ensure it is up to date and complete prior to the Operational Period Briefing and plan distribution.
  - Provide the IAP briefing plan, as required, and distribute the plan prior to the beginning of the new Operational Period.
- The Documentation Unit will normally be responsible for reproducing the IAP.
- The Resources Unit coordinates with the Logistics Section to acquire the amount and type of resources needed.
- The Incident Commander/Unified Command reviews and approves the IAP.

Key participants include:

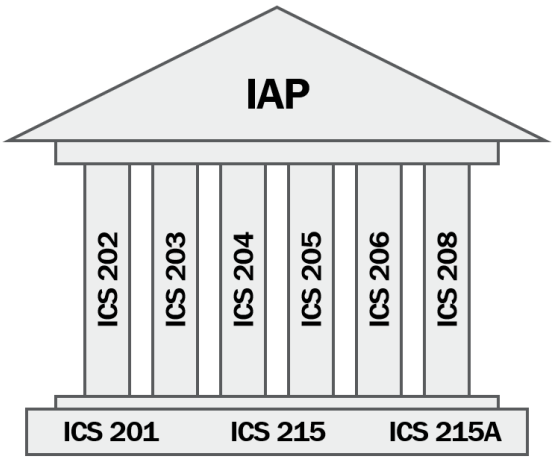
- Planning Section Chief
- Incident Commander

- Operations Section Chief
- Logistics Section Chief
- Safety Officer
- Finance/Administration Section Chief
- Communication Unit Leader
- Medical Unit Leader
- Liaison Officer
- Public Information Officer

IAP Components

The written IAP is a series of standard forms and supporting documents that convey the Incident Commander's and the Operations Section's directions for carrying out the plan for that Operational Period. The Planning Section Chief, with the approval of the Incident Commander, determines what components will be included in the Incident Action Plan for each operational period. The Planning Section Chief is then responsible for the completion and distribution of the IAP. Keep in mind that we only need to include content that helps Operations do their jobs safely and effectively and supports them. However, each jurisdiction may also have legal or policy-related mandates for planning efforts and documentation.

Figure 47: IAP Components



The IAP consists of ICS Forms 202, 203, 204, 205, 206, and 208. ICS Forms 201, 215, and 215A are not part of the IAP but may be provided as supporting information.

- Incident Objectives (ICS Form 202) – what is to be done
- Organization Assignment List (ICS Form 203) – who is assigned
- Assignment List (ICS Form 204) – what they are assigned to do
- Incident Radio Communications Plan (ICS Form 205) – how we talk to each other
- Communications List (ICS Form 205A) (optional) – all methods of non-radio contact information for personnel assigned

- Medical Plan (ICS Form 206) – how to treat medical/injured responders
- Incident Organization Chart (ICS Form 207) (optional) – visual chart depicting organizational positions and who is assigned to each
- Safety Message/Plan (ICS Form 208) – how to keep people safe
- Incident maps, traffic plans, charts, FAQs, and other helpful information

It is a best practice to include a cover sheet to indicate which forms and supporting documents are included in the IAP. An alternate approach is to list the contents of the IAP at the bottom of the Incident Objectives (ICS Form 202). The key concept is that an IAP may not contain all ICS forms. The use of a checklist to indicate which forms and supporting documents are enclosed as part of the IAP will ensure that IAP users understand what forms were included.

It is also important to understand that an IAP will change over time in an incident. Initial IAPs may be shorter and response action-focused. Later, IAPs may be longer, contain more forms, and include recovery and mitigation objectives. Again, listing the components included in the IAP will help IAP users.

Additional supporting documents may include weather forecasts, incident traffic plan, showing ingress and egress routes for resources, and other important information for operational supervisors.

IAP Components and Preparers

IAP Component	Normally Prepared By
Incident Objectives (ICS Form 202)	Incident Commander or Unified Command
Organization Assignment List or Chart (ICS Forms 203, 207)	Resources Unit Leader
Assignment List (ICS Form 204)	Resources Unit Leader
Incident Radio Communications Plan (ICS Form 205) Or Communications List (ICS Form 205A)	Communications Unit Leader
Medical Plan (ICS Form 206)	Medical Unit Leader
Incident Maps	Situation Unit Leader
General Safety Message/Site Safety Plan (ICS Form 208)	Safety Officer

Other Potential IAP Components	(Incident Dependent)
Air Operations Summary	Air Operations Branch Director
Traffic Plan	Ground Support Unit Leader
Decontamination Plan	Technical Specialist
Waste Management or Disposal Plan	Technical Specialist
Demobilization/Deactivation Plan	Resources Unit Leader, 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 Leader
Sheltering/Mass Care Plan	As needed
Other (as needed)	As needed

IAP Approval and Distribution

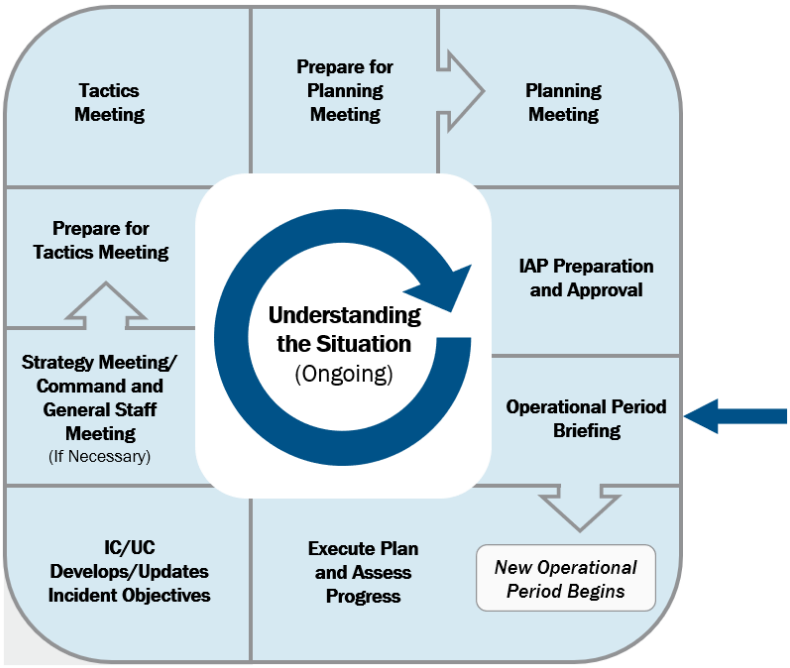
Based on concurrence from all elements at the end of the Planning Meeting, the Incident Commander or Unified Command approves the Incident Action Plan. After this final approval, the Planning Section staff assembles the plan and ensures that it is ready for use during the Operational Period Briefing.

Distributing the IAP for an Operational Period Briefing

- Approach varies with the situation as well as the number of personnel and copies.
- Consider using a QR Code or other hyperlink for electronic access to the documents.
- Consider bundling (multiple copies as a single distribution) for certain divisions or groups.
- Limited Incident Action Plan numbers will require controlled distribution.
- Submit original and corrected Incident Action Plans to Documentation Unit Leader.
- Evaluate procedures and Incident Action Plan with your staff (make improvements or adjustments as necessary).
- Get ready to do it again.

Operational Period Briefing

Figure 48: Operational Period Planning Cycle – Operational Period Briefing



Purpose

The Operations Period Briefing is conducted at the beginning of each Operational Period, immediately before the start of the new operational period. Incident supervisory and tactical personnel receive the Incident Action Plan for the upcoming operational period during this briefing. During the briefing, the members of the Command and General Staff present the incident objectives, review the current situation, and share information related to communications and safety.

Remember that the Operational Period Briefing at the beginning of the new operational period is not the same thing as a shift change. Shift change is the transfer between one shift to another to ensure that incident personnel have opportunities to rest and rehabilitate between work periods. An operational period is the period of time set for the execution of a set of operational actions specified in the IAP. There may be multiple shifts and shift-change briefings within a single operational period. A shift change briefing is not an Operational Period Briefing.

Participants

The Operational Period Briefing presents the IAP to supervisors of the tactical resources to be employed during that period. Normally this will include Branch and Division/Group level

supervisors. Strike Team/Resource Team and Task Force leaders may also participate in this briefing, but it is more common for these leaders to be briefed on the IAP in a later, separate Division or Group briefing.

Key participants include:

- Planning Section Chief
- Incident Commander or Unified Command
- Operations Section Chief
- Logistics Section Chief
- Safety Officer
- Finance/Administration Section Chief
- Communication Unit Leader
- Medical Unit Leader
- Others may be included as necessary

In some cases, all of the tactical personnel may attend the Operational Period Briefing if this meets an operational need, and they can be accommodated. Keep in mind that this may be the first interaction between the ICS organization and operational supervisors. The ICS organization should present a positive first impression. The ICS leadership should demonstrate leadership, competence, and professionalism in their actions, as well as command presence. Their presentations should be organized, prepared, and concise. This will help to ensure that the tactical-level leaders gain confidence in the ICS organization.

Operational Period Briefing Agenda

The Operations Briefing should be concise; presenting the Incident Action Plan for the next operational period is the primary focus of the briefing. The Planning Section Chief facilitates the Operational Period Briefing and should create and follow a concise agenda. There is not a single set agenda for the Operational Period Briefing. Organizations have different approaches to the agenda for the meeting. A sample Operational Period Briefing Agenda is provided below.

Sample Operations Briefing Agenda

Agenda Item	Who Performs Action	Content Notes
1. Introduction and Welcome	Planning Section Chief	
2. Opening Comments and review of Any Emphasis Areas	Planning Section Chief (PSC)	
3. Review: • Current Incident/Objective Status • Incident Boundaries, Branch/Division Locations, and Group Assignments (Map) • Division/Group Assignments (Assignment List ICS Form 204)	Operations Section Chief (may include Technical Specialists as necessary)	Reviews all Division/Group Assignments (Assignment List ICS Form 204), ensuring supervisors thoroughly understand the tactical assignment, resources, communications, special instructions, and safety issues. • Note: It is not unusual for incident conditions to have changed between the time the IAP is duplicated and the operations briefing. The Operations Section Chief may dictate last-minute changes to the IAP.
4. Safety Issues, Safety Message/ Weather Outlook	Safety Officer/ Situation Unit Leader	Briefs safety issues such as accidents and injuries to date, continuing and new hazards, and mitigation efforts. Reviews Safety Message.

Agenda Item	Who Performs Action	Content Notes
5. Logistics (Communications and Medical Plans)	Logistics Section Chief (may include Communications Unit Leader/ Medical Unit Leader as necessary)	Reviews supply, transportation, food, and facilities-related issues. The Logistics Section Chief briefs (or may have staff brief) the following: • Medical Unit Leader presents the Medical Plan (ICS Form 206), ensuring that all supervisors understand the procedures to follow if a responder is injured in the incident. • Communications Unit Leader briefs the overall Incident Communications Plan (ICS Form 205) and Communications List (ICS Form 205A).
6. Other Staff	Incident Dependent (Finance/Admin Section Chief, Liaison Officer, Public Information Officer, etc.)	Other Personnel may review additional IAP elements as needed. These may include: • Air Operations Summary • Fiscal or Compensation/Claims issues • Issues associated with cooperating or assisting agencies • Media and incident information issues • Other issues (may include presentations by Training Specialist, the Demobilization Unit Leader, etc.)
7. Closing remarks	Agency Administrator and/or Incident Commander/ Unified Command	
8. Conclusion	Planning Section Chief	Briefs housekeeping information such as times of next meetings, etc., and concludes the meeting

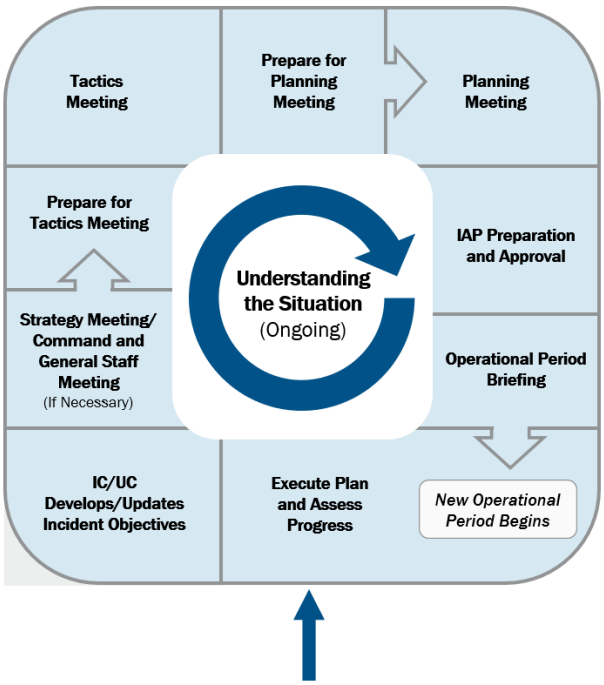
After the Operational Period Briefing

Following the Operational Period Briefing, supervisors brief their assigned personnel on their respective assignments as documented in the IAP. Staff members are briefed on the

operational elements of the plan to ensure they are aware of who they will work for and what it is that must be accomplished. In this briefing, staff members will have a chance to ask questions regarding the plan, any critical safety issues, and specific logistical information.

Execute the Plan and Assess Progress

Figure 49: Operational Period Planning Cycle – Execute Plan and Assess Progress



Purpose

This is the part of the operational period in which the approved plan is executed with the help of all other units and staff. It takes up a small portion of the diagram, but for many members of the ICS organization, this activity is what they will spend the majority of each operational period performing. Based on the designed operations, they perform tactical activities. Task Force and Strike Team leaders, in particular, spend most of their time performing the tactics that were approved to achieve the incident objectives defined in the Incident Action Plan. Along the way, success or impediments are documented so that in the next operational period, should the need arise, they can make adjustments to the plan.

Monitoring Incident Operations

Assessing Progress

The Operations Section directs the implementation of the plan. The supervisory personnel within the Operations Section are responsible for the implementation of the plan for the specific operational period.

The plan is evaluated at various stages in its development and implementation. Assessment is an ongoing, continuous process to help adjust current operations, as appropriate or required, and help plan future operations to meet the incident objectives. The plan is assessed at various stages, such as:

- First, all members of the Command and General Staff review the final plan document and correct any discrepancies.
- Next, during the implementation of the plan, all incident supervisors and managers must continually assess progress and the effectiveness of the plan based on the original measurable objectives for the operational period. This evaluation of the plan keeps responders on track and on task and ensures that the next operational period plan is based on a reasonable expectation of the success of the current plan. Remember the importance of the need to evaluate the status of the incident, e.g., severity or intensity of the incident, weather conditions, and other factors that might influence the success of the plan and, of course, the safety of the operators and community.
- Supervisors also monitor resource needs and adjust resources for evolving incident needs. This includes identifying which resources may need to be increased or which may need to be redeployed or demobilized.
- Finally, the Operations Section Chief may make the appropriate adjustments during the operational period to ensure that the objectives are met and effectiveness is assured. This helps determine the need for change in the current operational period or the next.

Monitoring Resource Needs

One of the benefits of the operational planning process is the ability to identify strategies, tactics, and resource requirements in advance. This planning process allows the Operations Section to align tactical operations and the appropriate resources. This also allows the Logistics Section to order resources as early as possible to help ensure that they are available for the next operational period.

During the current operational period, the Operations Section Chief must monitor the status of the incident and tactical reserves that are assigned to Staging Areas. If they reach “drawdown” levels during current operations, additional resources may need to be ordered, or tactics may need to be adjusted if they are unavailable.

During wildland fire season, hurricane season (both run concurrently), or other widespread incidents (e.g., pandemic, civil unrest), resources need to be monitored on a regional, statewide, and national level. Even with proactive planning and resource ordering efforts, critical resources may be delayed or not available at all.

Adjusting Resources to Evolving Incident Needs

Evaluation of resource performance involves monitoring, evaluating, and adjusting the performance of the organization and its components to ensure that all efforts are directed toward achieving the specified objectives.

Resources should be evaluated:

1. On an ongoing basis, as part of resource monitoring.
2. At demobilization, upon the achievement of the assigned tactical objectives. The Incident Personnel Performance Rating (ICS Form 225) may be used for the demobilization evaluation.
3. During after-action reporting.

If a resource is not the right response for a situation, then it should be replaced or augmented with a resource that best suits the need.

Determining the Need for a Change in Incident Objectives

The Incident Commander/Unified Command will determine if the incident objectives need to be adjusted, amended, or amended, based on the information provided by Command and General Staff members (particularly the Operations Section Chief). Here are some questions to consider when assessing objectives:

1. Is the incident stable, or is it increasing in size and complexity?
2. What are the current incident objectives, strategy, and tactics?
3. Are there any safety issues?
4. Are the objectives effective? Is a change of course needed?
5. How long will it be until the objectives are completed?
6. What is the current status of resources?
7. Are resources in good condition?
8. Are there sufficient resources?

If a change to the incident objectives is required, the Incident Commander/Unified Command will meet to draft the changes.

Chapter 8: Transition and Demobilization

Transition

Transition Plan

A transition plan is written by the current ICS organization to guide the incoming ICS organization or Agency Having Jurisdiction (AHJ) in assuming responsibility and accountability for the incident. The transition plan should be in a format that outlines what happened, actions taken, current situation, critical issues, priorities, and strategies moving forward. Each member of the current ICS organization is responsible for writing their piece of the narrative, explaining their specific positions, actions, and contributions so that the next person to fill the position understands their role. The plan should provide an organized cadence for the transitioning personnel and prevent any disruption in the incident status during the transition period.

Shift Changes

The Operational Period Briefing is referred to as the Operations Briefing by some ICS organizations. In some cases, the Operational Period Briefing occurs at the same time as a shift change and is incorrectly referred to as a shift change briefing. Remember that these are separate and distinct activities. The Operational Period Briefing delivers the IAP for the next operational period. The shift change allows personnel time to rest and refit between work assignments. Note that during longer operational periods, multiple shift changes may be conducted within an operational period. It is critical that information is relayed and that incoming resources are properly briefed at a shift change that may not coincide with the formal Operations Briefing. Safety may be compromised when information is not passed along properly. This briefing should be documented as well.

Documentation

The Activity Log (ICS Form 214) is key to refreshing your memory years later when a question or inquiry about the incident arises. Much like a police or fire report, it is utilized to determine what occurred on a certain date and time. Memories fade, and recollections get blurred. Document the important matters that will help you recall the day.

The Incident Status Summary (ICS Form 209) is a document of key facts and data that serve as a snapshot of the incident on a certain date and time. Most of the information is developed from key questions asked by stakeholders involved in incidents. Some of the forms may be oriented toward wildland fire, but we are seeing a shift toward utilizing the FEMA Lifelines as a vital way to capture relevant status information on a community.

Brief Your Supervisor on Status

Keeping your supervisor informed on how your work is progressing and how you are doing is vital to success. Long hours, frustration, fatigue, and a myriad of other matters come into play during a critical incident. Failure to keep the supervisor informed will delay much-needed assistance or downtime, affect job performance, and result in you and others getting hurt.

Communicate Status to Replacement

Resources should always brief their replacement in the same respect that any outgoing Incident Commander or other leaders would brief their replacement. What are the vital pieces of information that your replacement needs to know to be successful? These may include:

- Who do they answer to, and what is that supervisor like?
- What were your successes?
- Where are the "landmines?"
- How does the process work for requesting resources?
- Who are the key players and stakeholders?

Potential Risks to Avoid

Risks to avoid other than the non-safety type may include:

- Political "hot buttons"
- Not understanding local structures
- Internal and external rivalries
- Historical matters in the community
- Failure to integrate into local culture
- Dealing with egos

Transfer of Command

The transfer of command of an incident (TOC) can occur at several different points during an incident. From an external view of an outside ICS organization, the first transfer of command will usually occur when the command transfers from the initial IC to the Incident Commander/Unified Command from the outside ICS organization.

It is important to note that on many outside ICS organizational deployments, the local jurisdiction will retain "command" of the incident. The outside ICS personnel will be integrated into the response or recovery effort to augment or support the local resources. In these instances, the outside ICS organization will serve as an Incident Management Assistance Team or Incident Support Team, and transfer of command does not occur.

Transfer of command can also occur from one ICS organization to another ICS organization. This may happen if an ICS organization, such as a Type-3 IMT is replaced by a Type-2 or Type-1 ICS organization due to incident complexity. For IMTs, transfer of command may occur between IMTs when the original IMT comes to the end of their deployment period (times out) and has to demobilize before the incident is over. It is also possible for a Type-1 or Type-2 IMT to transition and transfer command to a Type-3 IMT or other ICS organization as the incident stabilizes.

Finally, transfer of command will occur when the incident concludes, the ICS organization is demobilizing, and the command returns to the home agency or jurisdiction.

Transitioning from Response to Recovery

A transition may happen in several ways. Some common transitions are from local jurisdiction to ICS organization, from ICS organization to ICS organization, or from ICS organization back to the local jurisdiction. In some cases, the ICS organization will be an Incident Management Team (IMT). Regardless of whether an IMT is involved, the process remains the same.

Much of the content for Transition and Demonization is taken from the National Disaster Recovery Framework (NDRF).

Shifting from Response to Recovery

All incidents go through phases from start to finish. We refer to these phases as initial response/attack, extended response/attack, activation, and operations. During this period, the incident will escalate, stabilize, and eventually be mitigated, and demobilization will occur. During large, complex incidents, we refer to it as the response and recovery phases of an incident.

The response phase is defined by life safety efforts, controlling/stabilizing the harm or threat, and protecting values at risk, e.g., the environment, critical infrastructure, property, etc. The recovery phase addresses the effects of the incident, supports life sustainment, and tries to return the community to normalcy.

Returning the Area to Its Previous State

Incident Commanders/Unified Commands should always be thinking about an “exit strategy” when deployed. Questions such as, “How good is good?” “How clean is clean?” “What does ‘right’ look like?” or “Can the community stand alone?” should help to determine when it is appropriate for the ICS organization to demobilize.

Full recovery after a serious incident may take years to complete. The Incident Commander/Unified Command must work with the Agency Administrator to determine when the incident is stabilized and when the community has sufficient capacity/capabilities to

stand alone and continue with the recovery effort. The Incident Commander/Unified Command must work closely with the Agency Administrator to ensure the team has met his/her priorities, needs, and expectations before demobilizing.

Network on Interconnected Entities

The recovery process is best described as a sequence of interdependent and often concurrent activities that progressively advance a community toward its planned recovery outcomes. Decisions made and priorities set by a community pre-disaster and early in the recovery process have a cascading effect on the nature, speed, and inclusiveness of recovery. Figure 53: Recovery Continuum depicts the interconnectedness of recovery activities from pre-incident through the long term. (NDRF, 2016)

From a Response ICS Organization to a Recovery ICS Organization

As stated earlier, ICS organizations are requested when an incident exceeds the capacity or capability of the community to effectively manage the incident. Some believe that the "incident" only applies to the response phase (e.g., life safety, incident control/stabilization, protection of values at risk). After that, their mission is complete, and the team should be demobilized.

In reality, the end of the response and the initial stages of the recovery run concurrently the majority of the time. Many communities are still devastated and struggling to provide for the community long after the response phase ends. As the life safety priority stabilizes, the equally important life sustainment mission emerges. This may include shelter operations, pet/animal care, points of distribution (POD) for food and water, public health protections, etc. Additionally, other important functions of the community, such as damage assessment, critical infrastructure restoration (e.g., utilities, medical, transportation), debris removal, business/economic recovery, etc., must be addressed.

ICS organizations should be prepared for the mission to assist with and support the short-term recovery (days) and initial phases of the intermediate recovery (weeks to months) efforts. This may include continuing the deployment past the response phase or beginning a mission strictly to support the initial recovery until the community can undertake the effort without assistance.

Typically, incident response deployments last for several days up to two weeks, depending on the incident and community. Depending on the duration of the assignment, a second ICS organization may have to transition with the initial ICS organization to continue to manage and support the recovery effort.

From a Response ICS Organization to the Local Jurisdiction

The Incident Commander/Unified Command must work closely with the Agency Administrator to ensure the team has met his/her priorities, needs, and expectations to the

best of their ability. Sometimes the Incident Commander/Unified Command may have to advocate for a longer stay to ensure the community is prepared to successfully manage the recovery process. At other times, the Incident Commander/Unified Command may have to assure the Agency Administrator that the community is capable of handling the effort.

Once the ICS organization is ready to demobilize, the standard closeout procedures will apply. The ICS organization should prepare for a clean transition back to the Agency Administrator and ensure they provide a solid plan and briefing for the Agency Administrator. It is important to identify efforts that have been completed and open items that still need to be addressed. The final document package will be very important as the community attempts to seek reimbursement for the response and recovery.

Using Community Lifelines to Guide Transition

The FEMA Community Lifelines are an excellent indicator of a community's position in regard to normalcy. Rather than focusing on just the response and life safety aspects of the incident, the Community Lifelines provide a much more global and holistic view of the situation and status of the community. Many of the community sectors are interconnected and dependent on each other for recovery success. ICS organizations should utilize the Community Lifelines as a reference point to help understand the full impact of the incident, especially during the recovery process.

For more information about FEMA Community Lifelines and also the Community Lifelines Toolkit, go to: https://www.fema.gov/emergency-managers/practitioners/lifelines

Foundational Components of Recovery Frameworks

This Framework guides recovery leaders and stakeholders by:

- Identifying guiding principles for achieving a successful recovery.
- Outlining pre- and post-disaster roles and responsibilities for recovery stakeholders and recommending leadership roles across all levels of government.
- Describing how the whole community will build, sustain, and coordinate the delivery of the Recovery core capabilities.
- Explaining the relationship between Recovery and the other mission areas (Prevention, Protection, Mitigation, and Response).
- Promoting inclusive and equitable coordination, planning, and information-sharing processes.
- Encouraging the whole community to leverage opportunities to increase resilience and incorporate climate adaptation and mitigation measures pre- and post-disaster, such as continuity planning, land use, and environmental regulations.

- Identifying scalable and adaptable organizations for coordinating recovery.
- Describing key factors, activities, and considerations for pre- and post-disaster recovery planning.
- Ensuring recovery resources are sourced from a wide range of whole community partners, including individuals and voluntary, nonprofit, philanthropic, and private sector and governmental agencies and organizations. (NDRF, 2016)

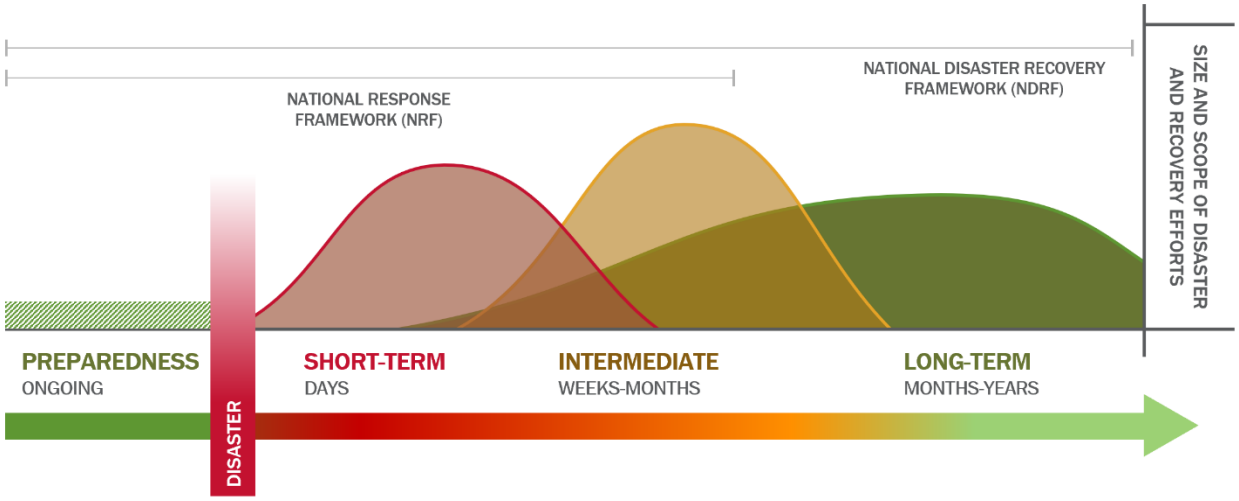
Guiding Principles

1. Individual and Family Empowerment
2. Leadership and Local Primacy
3. Pre-Disaster Recovery Planning
4. Engaged Partnerships and Inclusiveness
5. Unity of Effort
6. Timeliness and Flexibility
7. Resilience and Sustainability
8. Psychological and Emotional Recovery

Recovery Continuum

The Recovery Continuum highlights the reality that disaster preparedness, response, and recovery are not and cannot be separated from sequential efforts when a community faces significant and widespread catastrophe impacts (NDRF, 2016). Laying an effective foundation for recovery outcomes is a key requirement of response activities, but planning for recovery begins before a response. Community-level planning for recovery is a preparedness-phase activity that strengthens continuity and response and hastens recovery. The challenge is to ensure adequate and effective coordination between different efforts and players, as the decisions and outcomes for all phases are interconnected. An example is a major employer deciding to relocate rather than rebuild because it perceives that destroyed housing, roads, retail, and basic government services are not being restored and rebuilt timely and adequately. This outcome may have been avoided by including the employer in pre- and post-disaster recovery planning efforts and maintaining close coordination after the incident.

Figure 50: Recovery Continuum



Core Capabilities

The recovery core capabilities are:

Planning

Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.

Public Information and Warning

Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard and, as appropriate, the actions being taken, and the assistance being made available.

Operational Coordination

Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Economic Recovery

Return economic and business activities (including food and agriculture) to a healthy state and develop new business and employment opportunities that result in an economically viable community.

Health and Social Services

Restore and improve health and social services capabilities and networks to promote the resilience, independence, health (including behavioral health), and well-being of the whole community.

Housing

Implement housing solutions that effectively support the needs of the whole community and contribute to its sustainability and resilience.

Infrastructure Systems

Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

Natural and Cultural Resources

Protect natural and cultural resources and historic properties through appropriate planning, mitigation, response, and recovery actions to preserve, conserve, rehabilitate, and restore them consistent with post-disaster community priorities and best practices and in compliance with applicable environmental and historic preservation laws and executive orders.

Demobilization

Demobilization is the planned and systematic release of resources from an incident or event. Demobilization is based on a Demobilization Plan developed by the Planning Section with input from the C&GS members and approval by the Incident Commander/Unified Command. An organized process enhances the safe release of resources, accountability of personnel and equipment, and fiscal management.

Demobilization of resources may occur for the following reasons:

- Resources have completed their mission and are no longer needed (e.g., specialized USAR teams).
- Resources have reached the end of their deployment period and are “timing out.”
- The incident is stabilizing, and not as many resources are required.
- Emergency demobilization (e.g., an individual who has a personal emergency and must return home).

Demobilization may occur at any time during the life cycle of the incident/event.
The goal of demobilization is the orderly, safe, and efficient release and return of incident resources to their 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.

Importance

Demobilization involves all elements of the incident command organization. Demobilization will occur throughout the incident and in accordance with the Demobilization Plan. Demobilization procedures and priorities need to be understood by Command and General Staff early in the incident.

The Demobilization Unit Leader is responsible for the safe and orderly release of all resources from the incident or site. Resources may be demobilized before the completion of the incident for a variety of reasons.

Generally, we do a good job of mobilizing resources but find that demobilizing resources can be more challenging. Demobilization might pose an increased risk to the safety of the mission in that resources are fatigued, and equipment has deteriorated.

Timing

To many people, demobilization may seem like the anti-climactic part of the incident as everyone is ready to go home. It is the Demobilization Unit Leader's task to keep everyone motivated to get things back in their place and complete the required documentation. Also, everyone is usually very tired during demobilization, and there is a higher risk of accidents. Personnel must have enough rest before getting on the road after demobilization. Agencies may provide directions regarding which resources to release. Contractual obligations could include heavy equipment limitations or union contracts. Cost containment requirements are very high profile. However, the most important priority is meeting the needs of the incident.

Monitoring Resources

Leaders at every level of the response need to track the availability and status of resources that they are responsible for. This information must be accurate and reported through the chain of command to the Resource Unit Leader. Some of the information that leaders will need to report include:

- Kind, type, and numbers
- Constraints and capabilities
- Rest and work status

The status should reflect whether these resources are:

- Assigned (checked in and assigned work tasks on the incident)
- Available (checked in and ready for specific work detail or function)
- Out of Service (checked in but unable to function for mechanical, rest, or personal reasons, or because their condition makes them unusable)

While the Resource Unit Leader is responsible for tracking and monitoring the changes in the status of resources, it is the responsibility of all personnel to participate in monitoring

the health and safety of everyone assigned to the incident. Anyone can report changes to the health and safety of personnel through the proper chain of command. As soon as the report is received, the Resource Unit Leader will take the appropriate steps in changing the status of the resources.

Reporting Excess Resources

Most resources on an incident will be assigned to the Operations Section to allow them to perform the tactics necessary in satisfying the incident objectives. The Resources Unit Leader will work with the Operations Section Chief to identify the required number of resources. Shortages or excesses of the required resources are determined by comparing the resources on hand to what the Operations Section requires to do the work. The Resources Unit Leader will coordinate with all other Command and General Staff in identifying/determining excess staff personnel. The Resources Unit Leader can assemble a tentative demobilization list of resources; however, this list will be fluid because any changes in the incident status can cause demobilization to be halted. If responders on the list have specific qualifications that are needed on the incident, they may be removed and reassigned to fill the immediate need rather than order a new resource.

Communicating Demobilization Plans to Staff

When writing the Incident Demobilization Plan, it is essential that the Demobilization Unit Leader coordinates with:

- Agency Dispatch/Coordination Center for concurrence
- Command and General Staff members
- Agency Representatives

The Demobilization Unit Leader coordinates with Section Chiefs to determine the specific demobilization procedures that are necessary to meet each Section's needs. Agencies may provide directions regarding which resources to release. The most important priority is meeting the needs of the incident and ensuring that resources demobilized from the incident safely return to their home jurisdiction.

Sometimes emergency demobilization is necessary for medical reasons, personal emergency at home, or disciplinary reasons. The Demobilization Unit Leader should have a plan established for the demobilization of resources in an emergency.

The Demobilization Unit Leader is responsible for reviewing incident resource records, notifying resources of their demobilization date and time, and evaluating logistics and transportation capabilities. The Demobilization Unit Leader will work closely with Logistics to ensure a smooth and timely release of resources.

When the Demobilization Plan is approved by the Incident Commander, it is distributed to:

- Incident Commander
- Command and General Staff
- All check-out locations
- Demobilization Centers (if applicable)
- Area Command (if applicable)
- Emergency Operations Centers (if applicable)

The Demobilization Unit Leader will ensure that copies of the Demobilization Plan are posted in prominent locations so all interested people can see the information. Distribute the plan no less than 24 hours before the first anticipated releases. The sooner the plan is handed out, the better. It allows Unit Leaders to begin planning for the release of their resources and allows all Sections/Units time to understand their specific responsibilities.

The primary roles of the Incident Commander and the Sections in demobilization planning are:

- Incident Commander: Approves resource orders and demobilization.
- Operations Section: Identifies operational resources that are, or will be, excess to the incident and prepares a list for Demobilization Unit Leader.
- Planning Section: Develops and implements the Demobilization Plan.
- Logistics Section: Implements transportation inspection program and handles special transport needs.
- Finance/Administration Section: Processes claims, time records, and incident costs and assists in release priorities.

Glide Path

In preparing for demobilization, a “glide path” is utilized to determine when resources should be released from the incident. This orderly process ensures that resources are available for continued operations but are not in excess and underutilized.

Glide Path is a tool used by the Resources Unit to document when resources assigned to an incident will “time out” and forecast when replacement resources will need to be ordered to maintain required staffing levels. The Resources Unit Leader will work closely with the Operations Section Chief and other supervisors to determine their projected needs compared to current resources.

Figure 51: Demobilization Glide Path Example

Glide Path Matrix for the "Fictional Incident" Division Supervisors

10 Division/Group Supervisors currently required

January	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Name														
Dax Ward	1	1	1	1	1	1	1	1	1	1	T			
Aileen Yates	1	1	1	1	1	1	1	1	T					
Maya Ayers	1	1	1	1	1	1	1	1	1	1	1	1	1	T
Paloma Andy	1	1	1	1	1	1	T							
Lola Cantrell	1	1	1	1	1	1	1	1	1	T				
Antwan Roth	1	1	1	1	1	1	1	1	1	1	1	T		
Brett Martin	1	1	1	1	T									
Kaylie Under	1	1	1	1	1	1	1	T						
Elianna Mayer	1	1	1	1	1	1	1	1	1	1	1	1	T	
Lynn Corman	1	1	1	1	1	1	1	1	1	1	1	1	1	T
A. Nguyen			1	1	1	1	1	1	1	1	1	1	1	T
B. Doe						1	1	1	1	1	1	1	1	T
C. Alvarez							1	1	1	1	1	1	1	T
	10	10	11	11	10	11	11	10	9	8	7	6	5	0

T represents the day a person would be required to travel; therefore, they are not available that day.
On January 3 and 4, the number goes above 10 to allow for debriefing time
If no additional resources are requested, there will be no Division Supervisors on January 14.

Final Documentation

It is always important to remember that the ICS organization is working for the Agency Administrator(s) during the response. As such, all of the documentation belongs to the incident. This includes original hard copy/paper documents, digital documents (emails, portable hard drive, etc.), maps/displays, etc. This final document package will be submitted to the Agency Administrator at the closeout meeting when the last assigned ICS organization demobilizes. The ICS organization should establish and maintain a documentation management process from the beginning of the incident so that it is not a monumental task near the end of the incident. The National Wildland Fire Coordinating Group (NWCG) has established a system for managing and storing incident documentation. While all-hazard IMTs do not need to adhere to this system, it is considered a "best practice" and one to reference and potentially emulate. One of the factors that ICS organizational performance is evaluated on is document/record management and thoroughness.

At the same time, members of ICS organizations will have to complete their agency and personal documentation once they demobilize and return home. This includes:

- Timesheets and payroll documentation
- Travel reimbursement documentation
- Copies of injury reports or compensation claims
- Training records, completed PTBs, performance evaluations, etc.
- Retain your own personal copy of ICS-214s and other incident notes

Final Incident Package

The Final Incident Package leaves a legacy regarding the performance of the ICS organization. A team that performs well on the incident but leaves a poor-quality package cannot be said to have been fully successful. The Final Incident Package is the long-term (lasting) impression that your ICS organization leaves. The records will be used for years after the ICS organization turns over responsibility for the incident.

The Final Incident Package is the compilation of all critical documents placed in the Incident File by the ICS organization during their assignment on the incident. Requirements should be provided to the ICS organization at the Agency Administrator Briefing.

The package is essential for the agencies responsible for following up on fiscal matters, meeting obligations agreed upon during the incident, addressing litigation, and performing other important management considerations.

The Planning Section Chief is primarily responsible for supervising the coordination and assembly of the package. All Command and General Staff are responsible for the preparation of their portions of the incident file for inclusion in the Final Incident Package.

The package is a chronological list of everything that has occurred. It is typically a collection of narrative reports from Unit Leaders that describe what was done, what the obstacles were, and the actions that were taken.

The agency administrators and staff receive a Close-Out Briefing that provides the following information:

- Incident summary
- Discussion of major events within the incident that may have lasting ramifications
- Turnover of appropriate incident documentation, including components that are not finalized
- An opportunity for agency administrators to bring up concerns before the incident's ending
- A final evaluation of incident management by the Agency Administrator/Senior Official

The Final Incident Package is the product created by the ICS organization that leaves a legacy regarding the performance of that ICS organization. It is essential for the agencies responsible to follow up on fiscal matters, meet obligations agreed upon during the incident, address litigation, and perform other important management considerations.

The Final Incident Package should conform to the following standards:

- Stored in standard, labeled file box and map tubes
- Checked to make sure all forms are legible
- Indexed
- Neat and well-organized
- Duplicate copies are eliminated if one would serve the need for documentation
- Placed in standard office storage file boxes and map tubes

In addition to the hard copies, maintain electronic files and include them with the final incident package. The Final Incident Package is then delivered with appropriate guidance to the Agency Administrator/Senior Official after the incident.

Planning and Preparing for Demobilization

Based on direction from the Resources Unit Leader, the Status/Check-in Recorder may assist the Demobilization Unit Leader in activities necessary to plan and prepare for the demobilization effort, such as:

- Setting up the physical needs of the Demobilization Unit (e.g., telephone extension(s), desks, information center, bulletin board(s), public address system, FAX machine, identifying transportation pick-up points)
- Grouping resources by similar characteristics (e.g., final destination, home state, logical travel routes, shared transportation means, common excess times)
- Preparing Demobilization Check-Out (ICS Form 221) for each resource with as much information as is known at the time and filing in alphabetical or sequential order by request number
- Collecting demobilization plan information (e.g., telephone numbers of ICP, incident dispatch, radio frequencies for travel check-in purposes, local offices to contact en route if an emergency arises, restricted travel information for wide loads, staging center location, and contact information, moving hazardous materials)
- Collating grouped information into logical lists that display tentative releases by date, time, location, travel method, etc.
- Transferring approved and scheduled resource departure information onto bulletin board displays, announcing via a public address system, or searching out and personally contacting resources to notify them of release plans

Resource Check-Out

Based on directions from the Resources Unit Leader, you may assist the Demobilization Unit Leader with activities necessary for checking out resources, such as:

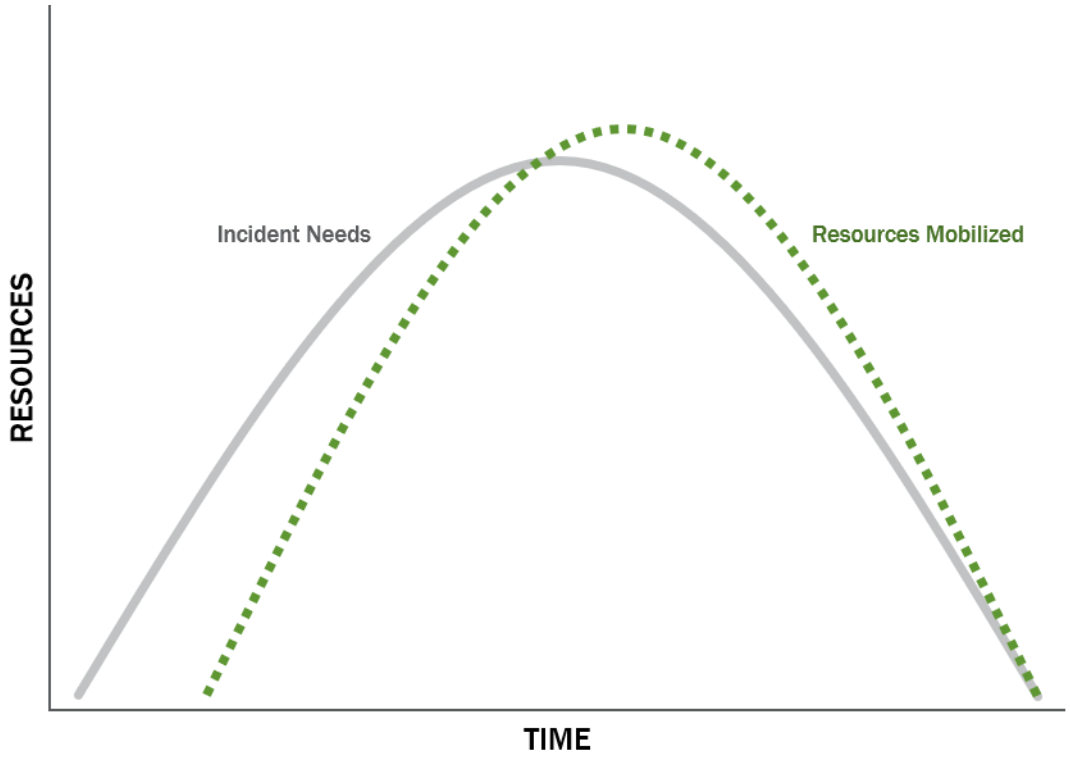
- Staffing the demobilization desk and providing completed Demobilization Check-Out (ICS Form 221) forms to release resources along with specific instructions regarding contact points at the ICP or incident base to complete the check-out process
- Interviewing resources having their own transportation to document estimated time of departure, estimated stops en route, and the estimated time of arrival at the home unit so that the home agency dispatcher can be notified
- Confirming travel information for resources not having their own transportation, such as type of travel, connecting travel types and times, estimated time of departure, estimated time of arrival, etc.
- Informing resources of any travel concerns or restrictions such as arriving at the destination before a certain time of day, not driving more than a certain number of hours, maintaining an awake passenger to keep the driver alert, mandatory rest breaks and/or check-in calls, need for sack lunches, etc.
- Documenting actual time of departure and collecting completed Demobilization Check-Out (ICS Form 221)

Notifying the Resources Unit, incident dispatch, and the resource's home unit of the actual time of departure, travel method and times, and the estimated time of arrival at home base by the communication method requested by the Demobilization Unit Leader.

Relationship Between Resources and Availability

The following graphic shows the relationship between incident resource needs and resource availability. In the beginning, more resources are needed than available. Later, the resource needs to catch up, and a surplus may exist until demobilized.

Figure 52: Relationship Between Resources and Availability



Identifying surplus resources and establishing a release order of resources requires constantly conferring with the Operations Section Chief and other Command and General Staff members.

Other factors when considering demobilization are:

- Obtain input from other agencies regarding the release of their resources by agency representatives
- Consider demobilizing resources from out of the area that will require contract carriers for their transportation and will save money in air carrier cost
- Consider banding resources from the same geographical area
- Demobilize the most expensive excess equipment and resources first unless the agency direction in the Demobilization Plan does not want to use this criterion for release priorities. Less expensive equipment may yield good performance

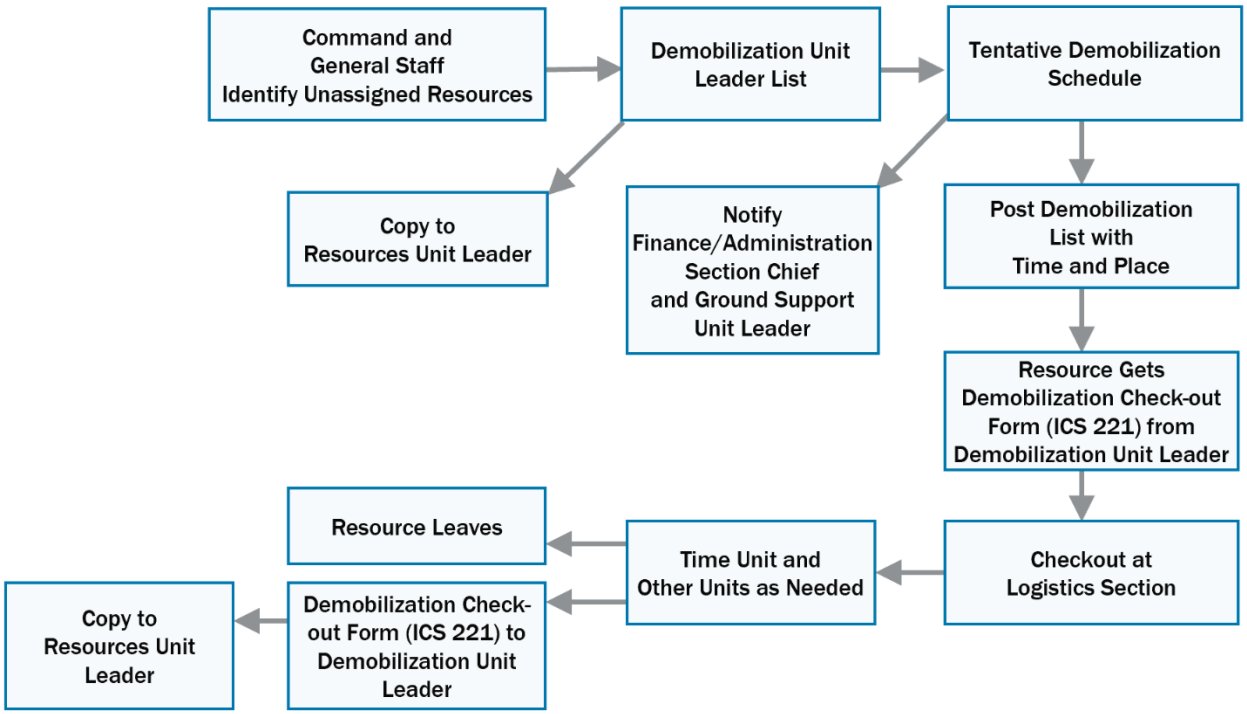
Demobilization can occur at locations other than the incident base (i.e., Demobilization Centers or Staging Areas). Here are some factors to consider:

- The condition of personnel
- Agency policy and memorandums of understanding (MOUs)
- The length of time on assignment(s)
- Fatigue and special needs
- The last rest period

Demobilization Process Workflow

Figure 53 is a roadmap of a sample Demobilization Plan and associated processes. It should be the responsibility of the Planning Section Chief and Demobilization Unit Leader to determine whether it will work for the respective incident and whether it follows the approved demobilization plan. Each team needs to determine what is appropriate for their incident.

Figure 53: Demobilization Process Workflow



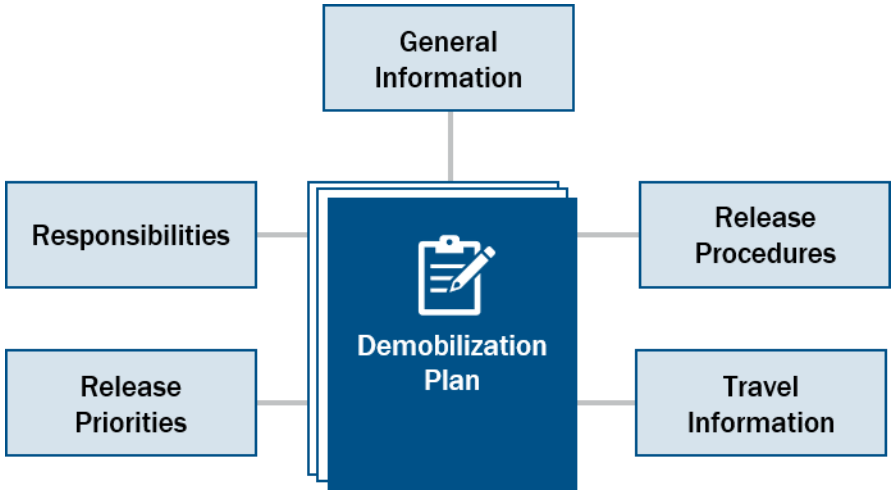
Demobilization Plan and Forms

The ICS 221 Demobilization Checkout list and the Formal Demobilization Plan are vital tools for a successful demobilization. The Demobilization Plan identifies procedures for demobilization as well as local, regional, and national priorities.

Sections of the Demobilization Plan include:

- General information about the demobilization process
- Responsibilities for the implementation of the Demobilization Plan
- General release priorities
- Specific release procedures
- Travel information (maps, telephone listings, etc.)

Figure 54: Sections of the Demobilization Plan



Performance Evaluations/PTBs

During the demobilization phase of the incident that occurs when a resource is released from the incident, supervisors must:

- Evaluations. The Incident Personnel Performance Rating (ICS Form 225) is generally prepared by the supervisor for each subordinate, using the evaluation standard given in the form. The Incident Personnel Performance Rating form will be reviewed with the subordinate, who will sign at the bottom. It will be delivered to the Planning Section before the rater leaves the incident.
- PTBs should be completed for tasks demonstrated during the incident. This also includes the evaluation portion of performance in the PTB.

Transition Meetings/Transition Plans

At some point, large, complex incidents wind down to a point where an external ICS organization is no longer needed, but the incident still needs attention. Often this is accomplished by releasing an external ICS organization and assigning local personnel to close out the incident. This process needs to be done in an orderly process to ensure safety and that nothing is lost or is not managed properly. There must be close coordination between the ICS organization and Agency Administrator/Executive.

Returning the incident to local management should be done as a team, not by individual team members. You may need to leave a Finance or Logistics person to help with remaining problems, settle unresolved claims, and assist in shipping equipment to caches. Don't take shortcuts or leave jobs undone. Be thorough. If some details are left undone, leave sufficient trucks. Don't leave a demobilization problem(s) for locals to resolve.

The purpose of these meetings is to ensure that the local Agency Administrator has all of the information and documentation that they need to continue with operations and move fully into recovery. Likewise, getting feedback and an evaluation of the team's efforts is valuable to the ICS organization.

Hot Washes

A "hot wash" is a facilitated discussion held immediately after an exercise among exercise players from each functional area. It is designed to capture feedback about any issues, concerns, or proposed improvements team members may have about the incident response. The hot wash is an opportunity for members to voice their opinions on the overall team response and their own performance. This facilitated meeting allows members to participate in a self-assessment of the response and provides a general assessment of how the jurisdiction performed in the response. At this time, evaluators can also seek clarification on certain actions and what prompted players to take them. Facilitators should take notes during the hot wash and include these observations in their analysis. The hot wash should last no more than 30 minutes.

This facet of response is critical so that the voices of all of the team members may be heard and issues discussed. From these notes, representatives with more formal After-Action Reports (AAR) will be able to further address matters focusing on the recognition of effectiveness or resolution of issues.

After Action Reports (AARs)/Improvement Plans (IPs)

During the post-incident phase of the incident (which occurs after a resource has been released from the incident and returned to home base), supervisors must lead an After-Action Review (AAR) with their teams. The AAR is a debriefing designed to get people to talk about what happened during the incident.

An AAR focuses on both the successes and failures of individuals and the team, and the goal is to learn from the experience and ensure that performance improves during subsequent incidents.

An After-Action Review answers the following questions:

- What did we set out to do?
- What actually happened?
- Why did it happen?

- What are we going to do differently next time?
- Are there lessons learned that should be shared?
- What follow-up is needed?

Through improvement planning, organizations take the corrective actions needed to improve plans, build and sustain capabilities, and maintain readiness. These are documented efforts with assignment of actions to specific parties for resolution with deliverables and timeframes attached.

Check Out/Team Evaluations

An ICS organization's performance evaluation should be based on objectives and direction provided by the Agency Administrator/Executive and the ICS organization's ability to achieve strategic and tactical implementation. This is a vital part of the closeout meeting with the Agency Administrator/Executive.

Factors considered in a written evaluation of an ICS organization include:

- Compliance with the Delegation of Authority
- Compliance with laws and regulations
- Compliance with Agency Administrator/Executive directions
- Orderly transition; local unit to team and team to local unit
- Human resource management
- Personnel safety records
- Financial performance compared to situational analysis predictions
- Accountability and control of all accountable property
- Documentation of incident costs
- Completeness of claims investigations and documentation
- Media relations
- Interaction with cooperative agencies/office staff/neighbors
- Effectiveness of suppression damage rehabilitation
- Orderly demobilization
- Completeness of final incident package

Evaluations are not intended to criticize team performance. They are intended as a constructive review of both the strengths of the team and areas for improvement.

Best Practices

Best practices in demobilization include:

- Starting the planning and process early. It takes time to develop and implement the plan.

- Maintaining a Demobilization Plan template that can be modified and updated as necessary.
- Posting tentative demobilization release notices at least 24 hours in advance to provide adequate notification to the resources.
- Ensuring resources are thoroughly rested before they depart for home.
- Inspecting all equipment for damage before it leaves the site.
- Making sure that you receive all the equipment that was given to resources.
- Having staff stop by medical for a last check and/or give them follow-up information related to any potential exposures.
- Getting all of their documentation before they leave.
- Having a process in place to estimate and then adjust their last timesheet to include travel time.
- Ensuring there is a method for them to close the loop and notify their supervisor that they have returned home safely.

References

Department of Homeland Security (DHS). (2018). *Countering False Information on Social Media in Disasters and Emergencies.* https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf

Deployable Training Division (DTD) Joint Staff J7. (2019). *Joint Headquarters Organization, Staff Integration, and Battle Rhythm*. Vol 3. https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/jtf_hq_org_fp.pdf

FEMA Directive: Personnel Standards of Conduct, FEMA Directive 123-0- 2-1. (2020). https://www.usfa.fema.gov/downloads/pdf/nfa/fema-directive-123-0-2-1.pdf

FEMA Directive: Temporary Directive Transmittal. (2000). https://www.fema.gov/pdf/library/temp00_02.pdf

FEMA, Incident Action Planning Guide. (2015). Vol 1. https://www.fema.gov/sites/default/files/2020-07/Incident_Action_Planning_Guide_Revision1_august2015.pdf

IT Program Assessment Department of Homeland Security (DHS) Analysis and Operations (A&O) Common Operating Picture (COP). (2012). https://www.dhs.gov/xlibrary/assets/mgmt/itpa-ao-cop2012.pdf

Lencioni, Patrick. M. (2002). The Five Dysfunctions of a Team. Jossey-Bass.

Management Directorate, Department of Homeland Security. (2017). Instruction Manual 262-12-001-01, DHS Lexicon Terms and Definitions. Vol 2, pp 142 and 317. https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

National Disaster Recovery Framework (NDRF). (2016). Vol 2. https://www.fema.gov/sites/default/files/2020-06/national_disaster_recovery_framework_2nd.pdf

National Incident Management System (NIMS). (2017). https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf

Nikos A. (2018). Using Just in Time Training for Active Learning in The Workplace. https://www.talentlms.com/blog/just-in-time-training-workplace/

National Incident Management System (NIMS). Incident Complexity Guide. (2021). Planning, Preparedness, and Training. https://www.fema.gov/sites/default/files/documents/fema_draft-incident-complexity-guide.pdf

National Incident Management System (NIMS) NQS. (2019). Supplemental Guide for Coaches and Evaluators. https://www.fema.gov/sites/default/files/2020-05/fema_nims_nqs_supplemental_coaches-evaluators_0.pdf

National Incident Management System (NIMS) Guideline for NQS. (2017). pp. 3-7. https://www.fema.gov/sites/default/files/2020-05/fema_nims_nqs_guideline_0.pdf

Oxford Learner's Dictionary. (2021). https://www.lexico.com/definition/coordination

Substance Abuse and Mental Health Services Administration (SAMHSA). (2020). Warning Signs and Risk Factors for Emotional Distress. https://www.samhsa.gov/find-help/disaster-distress-helpline/warning-signs-risk-factors

U.S. Fire Administration (USFA). (2014). Incident Management Handbook in English. https://homeport.uscg.mil/Lists/Content/Attachments/2923/2014%20USCG%20Incident%20Management%20Handbook%20in%20English.pdf

U.S. Fire Administration (USFA)/National Fire Academy (NFA). (2016). Field Operations Guide. pp. 8-14. https://www.usfa.fema.gov/downloads/pdf/publications/field_operations_guide.pdf

Appendix A: Glossary

This appendix contains terms frequently used by FEMA, which should also be understood by Incident Management Team members.

For access to FEMA's online glossary, go to: https://www.fema.gov/about/glossary.

A

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 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.

B

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.

C

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 those 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 the incident management organization.

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 Incident Command System title for individuals responsible for the management of functional Sections: Operations, Planning, Logistics, Finance/Administration, and Intelligence/Investigations (if established as a separate Section).

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 Incident Command Post (ICP).

Command staff often include a Public Information Officer (PIO), a Safety Officer, and a Liaison Officer, who has 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 qualifications 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.

D

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's resources to its original location and status.

Department 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 a 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 the 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.*

E

Emergency: Any incident, whether natural, technological, or human-caused, that requires 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 take 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. An EOP describes how people and property will be protected; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available; and outlines how all actions will be coordinated.

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.*

F

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

Finance/Administration Section: The Incident Command System Section responsible for all administrative and financial considerations surrounding an incident.

G

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.*

H

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

I

Incident: An occurrence, natural or manmade, that necessitates a response to protect life or property. In NIMS, 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 are performed. The Incident Command Post 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 a 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) 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 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.

J

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, 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 over 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.

K

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.

L

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; an Indian 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 Incident Command System Section responsible for providing facilities, services, and material support for the incident.

M

Management by Objectives: A management approach, fundamental to NIMS, which 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. It can also be called the Policy Group.

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

Mutual Aid and 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 before, during, and/or after an incident.

N

National: Of a nationwide character, including the Federal, State, tribal, and local 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 the 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).

O

Officer: The Incident Command System 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 are generally 12 to 24 hours but can vary in length and span multiple days.

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 Incident Command System 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 people with like objectives. Examples include, but are not limited to, governmental departments and agencies, NGOs, and private sector entities.

P

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 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. 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.

R

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

Recovery Plan: A plan developed to restore an 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: Mechanism used 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 an EOC.

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

S

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

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

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. Incident personnel use their best judgment to determine the actual distribution of subordinates to supervisors for a given incident.

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 uniformly.

State: Used in NIMS 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, which 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 plan or direction selected 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 sometimes referred to as resource teams.

Supervisor: The Incident Command System 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.

T

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.

U

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 within the 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 directions 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.

W

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.

Appendix B: Abbreviations

ICS Position Title Abbreviations

CODE	POSITION TITLE	CATEGORY
AOBD	Air Operations Branch Director	Air Ops
AREP	Agency Representative	Command
ASGS	Air Support Group Supervisor	Air Ops
ATGS	Air Tactical Group Supervisor	Air Ops
COML	Communications Unit Leader	Logistics
COMP	Compensation/Claims Unit Leader	Finance
COST	Cost Unit Leader	Finance
DIVS	Division/Group Supervisor	Operations
DMOB	Demobilization Unit Leader	Planning
DOCL	Documentation Unit Leader	Planning
FACL	Facilities Unit Leader	Logistics
FDUL	Food Unit Leader	Logistics
FSC	Finance/Administration Section Chief	Finance
GSUL	Ground Support Unit Leader	Logistics
HAZM	Hazardous Materials Specialist	Operations
IC	Incident Commander	Command
LOFR	Liaison Officer	Command
LSC	Logistics Section Chief	Logistics

CODE	POSITION TITLE	CATEGORY
MEDL	Medical Unit Leader	Logistics
OPBD	Operations Branch Director	Operations
OSC	Operations Section Chief	Operations
PIOF	Public Information Officer	Command
PROC	Procurement Unit Leader	Finance
PSC	Planning Section Chief	Planning
RESL	Resources Unit Leader	Planning
SITL	Situation Unit Leader	Planning
SOFR	Safety Officer	Command
SPUL	Supply Unit Leader	Logistics
STAM	Staging Area Manager	Operations
STCR	Strike Team Leader Crew	Operations
TFLD	Task Force Leader	Operations
THSP	Heavy Equipment Technical Specialist	Logistics
TIME	Time Unit Leader	Finance
UC	Unified Command	Command

Other Common Abbreviations

ABBREVIATION	DEFINITION
AHJ	Authority Having Jurisdiction
ANSI	American National Standards Institute

ABBREVIATION	DEFINITION
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

ABBREVIATION	DEFINITION
IPAWS	Integrated Public Alert and Warning System
IRIS	Incident Resource Inventory System
ISM	Incident Support Model
IT	Information Technology
IWI	Incident Within an Incident
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
NOAA	National Oceanic and Atmospheric Administration
NRCC	National Response Coordination Center
NTAS	National Terrorism Advisory System
NWCG	National Wildfire Coordinating Group
NWS	National Weather Service

ABBREVIATION	DEFINITION
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

Appendix C: Governing and Supporting Documents

Note the documents listed in this appendix are examples of governing and supporting guidance and are not used by all agencies. Also, note that agencies are continually updating and creating new guidance thus newer versions of these documents may become available after the publication date of this Reference Guide.

ICS History and Features

The concept of ICS was developed more than thirty years ago, in the aftermath of a devastating wildfire in California. During 13 days in 1970, 16 lives were lost, 700 structures were destroyed, and over one-half million acres burned. The overall cost and loss associated with these fires totaled $18 million per day. Although all of the responding agencies cooperated to the best of their ability, numerous problems with communication and coordination hampered their effectiveness. As a result, Congress mandated that the U.S. Forest Service design a system that would "make a quantum jump in the capabilities of Southern California wildland fire protection agencies to effectively coordinate interagency action and to allocate suppression resources in dynamic, multiple-fire situations."

Link: https://www.fema.gov/txt/nims/nims_ics_position_paper.txt

National Incident Management System (NIMS)

Communities across the Nation experience a diverse set of threats, hazards, and events. The size, frequency, complexity, and scope of these incidents 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.

https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf

NIMS Training Guide

Emergency Management Institute (EMI) works in collaboration with the whole community to provide training in support of the NIMS Training Program. The Preparedness Branch coordinates EMI's NIMS training efforts with the National Integration Center (NIC) to integrate NIMS doctrine and training with whole community needs.

Link: https://training.fema.gov/nims/

National Response Framework (NRF)

The National Response Framework (NRF) is a guide to how the nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities.

The NRF is structured to help jurisdictions, citizens, non-governmental organizations (NGOs), and businesses:

- Develop whole community plans
- Integrate continuity plans
- Build capabilities to respond to cascading failures among businesses, supply chains, and infrastructure sectors
- Collaborate to stabilize community lifelines and restore services

Link: https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response

Training guide: https://www.fema.gov/sites/default/files/2020-07/fema_national-response-framework-training-guide_2019.pdf

National Disaster Recovery Framework (NDRF)

The National Disaster Recovery Framework (NDRF) enables effective recovery support to disaster-impacted states, tribes, territorial, and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. The NDRF focuses on how best to restore, redevelop and revitalize the health, social, economic, natural, and environmental fabric of the community and build a more resilient nation. The NDRF is a first step toward achieving a shared understanding and a common, integrated perspective to achieve unity of effort and to build a more resilient nation.

Link: https://www.fema.gov/emergency-managers/national-preparedness/frameworks/recovery

NWCG PMS 210-1 Wildland Fire Incident Management Field Guide – Ver. 2014

The Wildland Fire Incident Management Field Guide states, references, or supplements wildland fire incident management and operational standards established by the National Wildfire Coordinating Group (NWCG). Relationship to the Incident Response Pocket Guide and Emergency Responder Field Operations Guide. This field guide contains some information that is duplicated in the Incident Response Pocket Guide (IRPG) and the Department of Homeland Security, Federal Emergency Management Agency (FEMA), National Incident Management System Emergency Responder Field Operating Guide (ERFOG), but the documents have different purposes and user groups. This field guide is the standard NWCG incident management reference guide. The IRPG is the "wildland fire job aid and training reference for operational personnel from Firefighter Type 2 through Division Supervisor and Initial Attack/Extended Attack Incident Commander," and is primarily an initial responder's tool. The ERFOG "provides guidance designed to assist emergency response personnel in the use of the National Incident Management System (NIMS) Incident Command System (ICS) during incident operations" and is primarily a Command and General Staff tool.

Link: https://www.nwcg.gov/publications/210

USFA NFA Field Operations Guide

The content of the Field Operations Guide (FOG) is intended to provide guidance for the application of the Incident Command System (ICS) to any planned or unplanned event. Position descriptions, checklists, and diagrams are provided to facilitate that guidance. The information contained in this document is intended to enhance the user's experience, training, and knowledge in the application of the Incident Command System. All users must obtain proper ICS training at the level necessary to effectively utilize the System.

Link: https://www.usfa.fema.gov/downloads/pdf/publications/field_operations_guide.pdf

USCG Incident Management Handbook

The United States Coast Guard (CG) Incident Management Handbook (IMH) is designed to assist CG personnel in the use of the National Incident Management System (NIMS) Incident Command System (ICS) during response operations. The ICS program has adopted the motto Ordo e Chao – Order out of Chaos. The IMH is intended to be used as a reference job

aid for responders to provide a systematic response process bringing order out of the chaos of incident response. It is not a policy document but rather guidance for response personnel requiring judgment in application. The CG is a first responder at state, tribal, and local levels and should be prepared to work with additional response personnel from other federal, state, and local agencies, non-governmental organizations (NGOs), and commercial entities. Through the guidance in the IMH, CG response operations align with the NIMS and can:

- Create an ICS organization and standard processes that integrate federal, state, tribal, and local agencies, NGOs, and commercial entities into a CG response operation, as the lead federal agency.
- Integrate seamlessly into existing local, tribal, state, federal agencies, NGOs, and commercial entities' ICS, as a supporting agency.

Link:
https://www.atlanticarea.uscg.mil/Portals/7/Ninth%20District/Documents/USCG_IMH_2014_COMDTPUB_P3120.17B.pdf?ver=2017-06-14-122531-930

Appendix D: Origin and Use of ICS Forms

The Incident Command System (ICS) was developed in the 1970s following a series of catastrophic fires in California's urban interface. Property damage ran into the millions, and many people died or were injured. The personnel assigned to determine the causes of this disaster studied the case histories and discovered that incident failures could rarely be attributed to a lack of resources or failure of tactics.

What were the lessons learned? Surprisingly, studies found that incident failures were far more likely to result from inadequate management than from any other single reason. Weaknesses in incident management were often due to:

- Lack of personnel accountability, including unclear chains of command and supervision.
- Poor communication due to both inefficient uses of available communications systems and conflicting codes and terminology.
- Lack of an orderly, systematic planning process.
- No common, flexible, predesigned management structure that enables commanders to delegate responsibilities and manage workloads efficiently.
- No predefined methods to integrate interagency requirements into the management structure and planning process effectively.

ICS forms are intended for use as tools for the creation of Incident Action Plans (IAPs), for other incident management activities, and support and documentation of ICS activities. These forms are designed to include the essential data elements for the ICS process they address. The use of these standardized ICS Forms is encouraged to promote consistency in the management and documentation of incidents in the spirit of NIMS and to facilitate the effective use of mutual aid.

Personnel using the forms should have a basic understanding of NIMS, including ICS, through training and/or experience to ensure they can effectively use and understand these forms.

ICS Form Descriptions

ICS uses a series of standard forms and supporting documents that convey directions for the accomplishment of the objectives and distributing information. The standard ICS forms, titles, and descriptions are listed in this section.

For access to all standard ICS forms, visit the EMI ICS Resource Center website at: https://training.fema.gov/emiweb/is/icsresource/icsforms/

ICS Form 200: IAP Cover Sheet

Purpose. The IAP cover sheet provides specific information about the IAP. The incident IAP cover sheets must be consistent with and reflect FEMA standards. Logos for FEMA, the State, Tribe, and other UCG member organizations may be used on cover sheets and must be produced in black and white.

Preparation. Prepared by the Incident Commander or Planning Section Chief.

Distribution. Duplicated and distributed to Command and General Staff positions activated. All completed original forms must be given to the Documentation Unit Leader.

Note: Refer to Appendix E for a completed IAP example.

ICS Form 201: Incident Briefing

Purpose. The Incident Briefing provides the Incident Commander (and the Command and General Staff) with basic information regarding the incident situation and the resources allocated to the incident. In addition to a briefing document, the ICS Form 201 also serves as an initial action worksheet. It serves as a permanent record of the initial response to the incident. It is used when the incident transitions from Initial Action to an Incident Management Team, ICS Form 201 provides basic information regarding the incident status situation and resources allocated to the incident.

Preparation. The briefing form is prepared by the Incident Commander for presentation to the incoming Incident Commander along with a more detailed oral briefing.

ICS Form 202: Incident Objectives

Purpose. The Incident Objectives form serves as the first page of the IAP (after the cover page). It describes the basic incident strategy, incident objectives, command emphasis/priorities, and safety considerations for use during the next operational period.

Preparation. The ICS 202 is completed by the Planning Section following each Command and General Staff meeting conducted to prepare the Incident Action Plan (IAP). In the case of a Unified Command, one Incident Commander (IC) may approve the ICS 202. If additional IC signatures are used, attach a blank page.

ICS Form 203: Organization Assignment List

Purpose. The Organization Assignment List provides ICS personnel with information on the units that are currently activated and the names of personnel staffing each position/unit. It is used to complete the Incident Organization Chart (ICS Form 207) which is posted on the Incident Command Post display. An actual organization will be incident or event-specific. Not all positions need to be filled. Some blocks may contain more than one name. The size of

the organization is dependent on the magnitude of the incident and can be expanded or contracted as necessary.

Preparation. The Resources Unit prepares and maintains this list under the direction of the Planning Section Chief. Complete only the blocks for the positions that are being used for the incident. If a trainee is assigned to a position, indicate this with a "T" in parentheses behind the name (e.g., "A. Smith (T)").

ICS Form 204: Assignment List

Purpose. The Assignment list informs Division and Group supervisors of incident assignments. Once the Command and General Staff agree to the assignments, the assignment information is given to the appropriate Divisions and Groups.

Preparation. The ICS 204 is normally prepared by the Resources Unit, using guidance from the Incident Objectives (ICS 202), Operational Planning Worksheet (ICS 215), and the Operations Section Chief. In some jurisdictions, the Operations Section Chief may choose to prepare the 204 so that they can select teams and supervisors themselves. They do so with direct assistance and cooperation with the RESL. A 204 is developed for each Division or Group.

ICS Form 205: Incident Radio Communications Plan

Purpose. The Incident Radio Communications Plan provides information on all radio frequency or trunked radio system talkgroup assignments for each operational period. The plan is a summary of information obtained about available radio frequencies or talkgroups and the assignments of those resources by the Communications Unit Leader for use by incident responders. Information from the Incident Radio Communications Plan on frequency or talkgroup assignments is normally placed on the Assignment List (ICS Form 204).

Preparation. The ICS 205 is prepared by the Communications Unit Leader and given to the Planning Section Chief for inclusion in the Incident Action Plan.

ICS Form 205A: Communications List

Purpose. The Communications List records methods of contact for incident personnel. While the Incident Radio Communications Plan (ICS Form 205) is used to provide information on all radio frequencies down to the Division/Group level, the ICS Form 205A indicates all methods of contact for personnel assigned to the incident (radio frequencies, phone numbers, pager numbers, etc.), and functions as an incident directory.

Preparation. The ICS 205A can be filled out during check-in and is maintained and distributed by Communications Unit personnel. This form should be updated each operational period.

ICS Form 206: Medical Plan

Purpose. The Medical Plan provides information on incident medical aid stations, transportation services, hospitals, and medical emergency procedures.

Preparation. The ICS 206 is prepared by the Medical Unit Leader and reviewed by the Safety Officer to ensure ICS coordination. If aviation assets are utilized for rescue, coordinate with Air Operations.

ICS Form 207: Incident Organization Chart

Purpose. The Incident Organization Chart provides a visual wall chart depicting the ICS organization position assignments for the incident. The ICS Form 207 is used to indicate what ICS organizational elements are currently activated and the names of personnel staffing each element. An actual organization will be event-specific. The size of the organization is dependent on the specifics and magnitude of the incident and is scalable and flexible. Personnel responsible for managing organizational positions are listed in each box as appropriate.

Preparation. The ICS 207 is prepared by the Resources Unit Leader and reviewed by the Incident Commander. Complete only the blocks where positions have been activated, and add additional blocks as needed, especially for Agency Representatives and all Operations Section organizational elements. For detailed information about positions, consult the NIMS ICS Field Operations Guide. The ICS 207 is intended to be used as a wall-size chart and printed on a plotter for better visibility. A chart is completed for each operational period and updated when organizational changes occur.

ICS Form 208: Safety Message/Plan

Purpose. The Safety Message/Plan expands on the Safety Message and Site Safety Plan. It outlines safety message(s), priorities, and key command emphasis/decisions/directions, safety hazards and specific precautions to be observed during this Operational Period.

Preparation. The ICS 208 is an optional form that may be included and completed by the Safety Officer for the Incident Action Plan (IAP). The 208 is developed using the ICS 215A Safety Analysis Worksheet.

ICS Form 209: Incident Status Summary

Purpose. The Incident Status Summary is used for reporting information on significant incidents. In some jurisdictions, they may have a similar form that has been customized to meet their needs for information collection. Agencies or organizations may set their own reporting requirements. Therefore, ICS 209s should be completed according to each jurisdiction or discipline's policies, mobilization guide, or preparedness plans. It is recommended that consistent ICS 209 reporting parameters be adopted and used by

jurisdictions or disciplines for consistency over time, documentation, efficiency, trend monitoring, incident tracking, etc.

The ICS 209 summarizes incident information for staff members and external parties and provides information to the Public Information Officer for the preparation of media releases. The ICS Form 209 is designed to provide a "snapshot in time" to effectively move incident decision-support information where it is needed. It should contain the most accurate and up-to-date information available at the time it is prepared.

Preparation. Typically, ICS 209 forms are completed either once daily or for each operational period – in addition to the initial submission. Jurisdictional or organizational guidance may indicate the frequency of ICS 209 submission for particular definitions of incidents or all incidents. This specific guidance may help determine submission timelines when operational periods are extremely short (e.g., 2 hours) and it is not necessary to submit new ICS 209 forms for all operational periods. The exact design of the Situational Report may vary based on reporting requirements and needs of the incident and jurisdiction.

When an Incident Management Organization (such as an Incident Management Team) is in place, the Situation Unit Leader or Planning Section Chief prepares the ICS 209 at the incident. On other incidents, the ICS 209 may be completed by a dispatcher in the local communications center, or by another staff person or manager. This form should be completed at the incident or the closest level to the incident.

The ICS 209 should be completed with the best possible, currently available, and verifiable information at the time it is completed and signed. If electronic data is submitted with the ICS 209, do not attach or send extremely large data files. Incident geospatial data that is distributed with the ICS 209 should be in simple incident geospatial basics, such as the incident perimeter, point of origin, etc. Data file sizes should be small enough to be easily transmitted through available connections or other limited communications capabilities when ICS 209 information is transmitted electronically. Regular capabilities may be limited based upon infrastructure damage from the incident. Streamlining of information may be necessary to facilitate successful transmission. Any attached data should be clearly labeled as to format content and collection time and should follow existing naming conventions and standards.

ICS Form 210: Resource Status Change

Purpose. The Resource Status Change is used by the Incident Communications Center Manager to record status change information received on resources assigned to the incident. This information could be transmitted with a General Message (ICS Form 213). The form could also be used by Operations as a worksheet to track entry, etc.

Preparation. The ICS 210 is completed by radio/telephone operators who receive status change information from individual resources, Task Forces, Strike Teams, and Division/Group Supervisors. Status information could also be reported by Staging Area and

Helibase Managers and fixed-wing facilities. This information may be captured using electronic data recording systems rather than the ICS 210 form.

ICS Form 211: Incident Check-In List

Purpose. Personnel and equipment arriving at the incident can check in at various incident locations. Specific check-in locations on box 3 of the ICS Form 211 include Base, Staging Area, ICP, Helibase, and Other (e.x. incident site). Check-in consists of reporting specific information, which is recorded on the Check-In List (ICS Form 211). The ICS Form 211 serves several purposes: (1) records arrival times at the incident of all overhead personnel and equipment, (2) records the initial location of personnel and equipment to facilitate subsequent assignments, and (3) supports demobilization by recording the home base, method of travel, etc., for resources checked in.

Preparation. The ICS 211 is initiated at a number of incident locations including Staging Areas, Base, and Incident Command Post (ICP). Preparation may be completed by (1) overhead at these locations, who record the information and give it to the Resources Unit as soon as possible, (2) the Incident Communications Center Manager located in the Communications Center, who records the information and gives it to the Resources Unit as soon as possible, and (3) a recorder from the Resources Unit during check-in to the ICP. As an option, the ICS 211 can be printed on colored paper to match the designated Resource Status Card (ICS 219) colors. The purpose of this is to aid the process of completing a large volume of ICS 219s.

INCIDENT CHECK-IN LIST (ICS 211)

1. Incident Name: Liberty County Fairgrounds Incident	2. Incident Number:	3. Check-In Location (complete all that apply): ☐ Base ☒ Staging Area ☐ ICP ☐ Helibase ☐ Other	4. Start Date/Time: Date: 08/16/XX Time: 0700

Check-In Information (use reverse of form for remarks or comments)

5. List single resource personnel (overhead) by agency and name, OR list resources by the following format:							6. Order Request #	7. Date/Time Check-In	8. Leader's Name	9. Total Number of Personnel	10. Incident Contact Information	11. Home Unit or Agency	12. Departure Point, Date and Time	13. Method of Travel	14. Incident Assignment	15. Other Qualifications	16. Data Provided to Resources Unit
State	Agency	Category	Kind	Type	Resource Name or Identifier	ST or TF											
Co	Libe	OH	IM	4	Initial R		1	08/16/XX 0600	IMT 1	10	IMTColumbiaRegion@columbia.	Liberty County	Liberty County 8/16/xx 0500	Persona	IMT	N/A	Y
Co	Libe	LE	Pat	III	Liberty (		2	08/16/XX 0600	Sgt 1	11	xxx-xxx-xxx	Liberty County	Liberty County 8/16/xx 0500	LE Mark	Perimeter	LE	Y
Col	Cer	LE	Pat	III	Central		3	08/16/XX 0600	Sgt 2	15	xxx-xxx-xxx	Central City	Central City 8/16/xx 0500	LE Mark	Traffic Control	LE	Y
Col	Libe	LE	Inv	III	Liberty (	TF	4	08/16/XX 0600	LE 4	9	xxx-xxx-xxx	Liberty County	Liberty County 8/16/xx 0500	LE Mark	Invesitigations	LE	Y
Co	Libe	PW	Dar	III	Liberty (	TF	5	08/16/XX 0600	PW 1	7	xxx-xxx-xxx	Liberty County	Liberty County 8/16/xx 0500	County \	Damage Assessme-t	ACT-20	Y
Col	Libe	FIR	Stru	III	Liberty (	ST	6	08/16/XX 0600	FD 3	13	xxx-xxx-xxx	Liberty County	Liberty County 8/16/xx 0500	Fire Eng	Extinguishment	Fire	Y
Col	Libe	FIR	Res	III	Liberty (	ST	7	08/16/XX 0600	R 1	9	xxx-xxx-xxx	Liberty County	Liberty County 8/16/xx 0500	Fire App	Rescue	Fire	Y
Col	Libe	EM	EM	III	Liberty (	ST	8	08/16/XX 0600	EMS 1	9	xxx-xxx-xxx	Liberty County	Liberty County 8/16/xx 0500	ALS / BL	Triage, Treatment	EMS	Y

ICS 211	17. Prepared by: Name: Amani Cruz	Position/Title: PSC	Signature: _____	Date/Time: 08/16/XX 0900

ICS Form 213: General Message

Purpose. The General Message is used by the incident dispatchers to record incoming messages that cannot be orally transmitted to the intended recipients. The ICS Form 213 is also used by the Incident Command Post and other incident personnel to transmit messages (e.g., resource order, incident name change, other ICS coordination issues, etc.) to the Incident Communications Center for transmission via radio or telephone to the addressee. This form is used to send any message or notification to incident personnel that requires hard-copy delivery. The ICS 213 is used to document and track important information flow in an incident.

Preparation. The ICS 213 may be initiated by incident dispatchers and any other personnel on an incident.

ICS Form 213RR: Resource Request Message

Purpose. The Resource Request Message is utilized to order resources, track resource status, and assist with determining incident costs. This form is a modification of the standard ICS 213 but is designed for requesting resources versus information flow. Either form may be used, but the 213RR may make it easier to include all information needed for resource requests.

Preparation. The ICS 213 RR is initiated by the resource requestor and initially approved by the appropriate Section Chief or Command Staff. The Logistics and Finance/Administration Sections also complete applicable sections of the form.

ICS Form 214: Activity Log

Purpose. The Activity Log records details of notable activities at any ICS level, including single resources, equipment, Task Forces, etc. These logs provide basic incident activity documentation and a reference for an after-action report. The standard ICS 214 information may also be captured via electronic reporting systems in lieu of paper forms. These records also serve as formal documentation of an incident and can be referenced should there be questions at a later date about activities or actions taken in an incident. Those questions could come months or even years after the date in question.

Preparation. An ICS 214 can be initiated and maintained by personnel in various ICS positions as it is needed or appropriate. Personnel should document how relevant incident activities are occurring and progressing, or any notable events or communications. Supervisory personnel may complete one ICS 214 for a team of individuals as long as they are in close proximity to the personnel and can accurately document actions taken.

ICS Form 215: Operational Planning Worksheet

Purpose. The Operational Planning Worksheet communicates the decisions made by the Operations Section Chief during the Tactics Meeting concerning resource assignments and needs for the next operational period. The ICS Form 215 is used by the Resources Unit to complete the Assignment Lists (ICS Form 204) and by the Logistics Section Chief for ordering resources for the incident.

Preparation. The ICS 215 is initiated by the Operations Section Chief and often involves logistics personnel, the Resources Unit, and the Safety Officer. The form is shared with the rest of the Command and General Staff during the Planning Meeting. It may be useful in some disciplines or jurisdictions to prefill ICS 215 copies before incidents.

ICS Form 215A: Incident Action Plan Safety Analysis

Purpose. The Incident Action Plan Safety Analysis aids the Safety Officer in completing an operational risk assessment to prioritize hazards, safety, and health issues, and to develop appropriate controls. This worksheet addresses communications challenges between planning and operations and is best utilized in the planning phase and for Operations Section briefings.

Preparation. The ICS 215A is typically prepared by the Safety Officer during the incident action planning cycle. When the Operations Section Chief is preparing for the tactics meeting, the Safety Officer collaborates with the Operations Section Chief to complete the Incident Action Plan Safety Analysis. This worksheet is closely linked to the Operational Planning Worksheet (ICS 215). Incident areas or regions are listed along with associated hazards and risks. For those assignments involving risks and hazards, mitigations or controls should be developed to safeguard responders, and appropriate incident personnel should be briefed on the hazards, mitigations, and related measures. Use additional sheets as needed.

ICS Form 217A: Communications Resource Availability Worksheet

Purpose. The Communications Resource Availability Worksheet is used by the Communications Unit Leader to assist in determining frequency allocation.

Preparation. Cache radio frequencies available to the incident are listed on the form. Major agency frequencies assigned to the incident should be added to the bottom of the worksheet.

ICS Form 218: Support Vehicle/Equipment Inventory

Purpose. The Support Vehicle/Equipment Inventory provides an inventory of all transportation and support vehicles and equipment assigned to the incident. The information is used by the Ground Support Unit to maintain a record of the types and

locations of vehicles and equipment on the incident. The Resources Unit uses the information to initiate and maintain status/resource information

Preparation. The ICS 218 is prepared by Ground Support Unit personnel at intervals specified by the Ground Support Unit Leader.

ICS Form 219: T-Cards

Purpose. Resource Status Cards are also known as "T-Cards." They are used by the Resources Unit to record status and location information on resources, transportation, and support vehicles and personnel. These cards provide a visual display of the status and location of resources assigned to the incident. T-Card information may also be kept using electronic or other means by agencies depending on resources and technology available.

Preparation. Information to be placed on the cards may be obtained from several sources including, but not limited to:

- Incident Briefing (ICS 201)
- Incident Check-In List (ICS 211)
- General Message (ICS 213)
- Agency-supplied information or electronic resource management systems

ICS Form 220: Air Operations Summary

Purpose. The Air Operations Summary provides the Air Operations Branch with the number, type, location, and specific assignments of helicopters and air resources.

Preparation. The ICS 220 is completed by the Operations Section Chief or the Air Operations Branch Director during each Planning Meeting. General air resources assignment information is obtained from the Operational Planning Worksheet (ICS 215), which also is completed during each Planning Meeting. Specific designators of the air resources assigned to the incident are provided by the Air Support Group Supervisor. If aviation assets would be utilized for rescue or are referenced on the Medical Plan (ICS 206), coordinate with the Medical Unit Leader and indicate on the ICS 206.

ICS Form 221: Demobilization Check-Out

Purpose. The Demobilization Check-Out ensures that resources checking out of the incident have completed all appropriate incident business, and provides the Planning Section information on resources released from the incident. Demobilization is a planned process and this form assists with that planning. This form also serves as documentation of items returned and inspected prior to the departure of resources. It ensures fiscal accountability for any items checked out by responders.

Preparation. The ICS 221 is initiated by the Planning Section, or a Demobilization Unit Leader if designated. The Demobilization Unit Leader completes the top portion of the form

and checks the appropriate boxes in Block 6 that may need attention after the Resources Unit Leader has given written notification that the resource is no longer needed. The individual resource will have the appropriate overhead personnel sign off on any checked box(es) in Block 6 prior to release from the incident.

ICS Form 225: Incident Personnel Performance Rating

Purpose. The Incident Personnel Performance Rating is used by supervisors to evaluate subordinates on incident assignments. It is used only to rate an individual's performance on an incident or event.

Preparation. The ICS 225 is normally prepared by the supervisor for each subordinate, using the evaluation standard given in the form. The ICS 225 will be reviewed with the subordinate, who will sign at the bottom.

ICS Form 260: Resource Order

Purpose. The Resource Order form is used to maintain a documented trail of resource orders during an incident. The ICS 260 is critical as the Ordering Manager actually assigns order numbers (O, E, C, A) for each resource. The AOP or EOC then fills the order and advises the ICS organization on what specific resource is actually filling that specific order number or request. This is then provided to the RESL for inclusion in the IAP. Many times, Logistics will use a spreadsheet or other electronic format if available to track this information. The document assists with the tracking of a multitude of information related to resources.

Preparation. This form is prepared by the Supply Unit Leader or the Logistics Section Chief.

Other ICS Forms

In addition to the standard forms provided by FEMA, there are several authorized ICS forms developed by the United States Coast Guard (USCG). Several commonly used USCG ICS forms are listed and described below.

For access to standard Coast Guard Incident Command System (ICS) Authorized Forms, visit the United States Cost Guard CG-612 Directives and Publications Division website at: https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6/The-Office-of-Information-Management-CG-61/Forms-Management/ICS-Forms/.

ICS Form 230 CG: Daily Meeting Schedule

Purpose. The Daily Meeting Schedule records information about the daily scheduled meeting activities.

Preparation. This form is prepared by the Situation Unit Leader and coordinated through the Unified Command for each operational period or as needed. Commonly held meetings are already included in the form. Additional meetings, as needed, can be entered onto the form in the spaces provided. The time and location for each meeting must be entered. If any of these standard meetings (pre-populated on the form) are not scheduled, they should be crossed out. This form can be accessed directly at: https://media.defense.gov/2017/Jul/28/2001784744/-1/-1/0/ICS_230_CG.PDF.

ICS Form 233 CG: Incident Open Action Tracker

Purpose. The Incident Open Action Tracker is used by the Incident Commander/Unified Command (IC/UC) to assign and track tasks/actions to ICS organization personnel that do not rise to the level of being an Incident Objective. This form may help ensure that tasks are not forgotten or overlooked. It can serve as somewhat of a checklist for personnel.

Preparation. The Planning Section Chief (PSC) is responsible for maintaining the Open Actions Tracker for the IC/UC and typically utilizes the Documentation Unit Leader (DOCL) to assist in this form's development and updating. The PSC should ensure all Command and General Staff are prepared to discuss their assigned tasks/actions during the Command and General Staff and Planning Meetings. This form can be accessed directly at: https://media.defense.gov/2017/Jul/28/2001784751/-1/-1/0/ICS_233_CG.PDF.

ICS Form 234 CG: Work Analysis Matrix

Purpose. The Work Analysis Matrix is designed to help select the best strategies and tactics to achieve the operational objectives. The ICS-234 is a decision support tool that allows the OSC to identify, evaluate, and document viable and nonviable (weather, lack of resources, prohibited by AA, cost, etc.) strategies for the incident. The OSC will select primary and alternate strategies to meet the operational objectives. This allows the OSC to explain his/her rationale for selection to the IC/UC during the Planning Meeting. Additionally, the ICS-234 can be used to cross-reference with the operational objectives to ensure the OSC has selected strategies and tactics to address them.

The tactics from this form carry forward to the “Work Assignment” on the ICS-215 or can simply be posted on the ICS-215 instead of the Tactics column on the ICS-234. Another purpose of the ICS-234 is that it presents alternative (or what-if) strategies and tactics to respond to bad weather, sudden changes in operational conditions, etc. This form is simply a formalized version of how most OSCs tend to think to turn objectives into tactical fieldwork.

Preparation. The Work Analysis Matrix, if used, is usually completed by the Operations Section Chief and Planning Section Chief prior to or at the Tactics Meeting and presented along with the ICS-215 during the Planning Meeting. This form can be accessed directly at: https://media.defense.gov/2017/Jul/28/2001784756/-1/-1/0/ICS_234_CG.PDF.

ICS Form 236 CG: Tentative Release List

Purpose. The Tentative Release List is an optional form used by Command and General Staff to identify excess or surplus resources on the incident for the Demobilization Unit Leader.

Preparation. The Tentative Release List is prepared by the Command and General Staff after receiving input from their staff on any surplus resources at least 24 hours in advance of their anticipated demobilization time. The Resources Unit Leader will work with the Operations Section Chief to identify Operations resources. The list of identified surplus resources is given to the Section Chief/Command Staff Officer who will sign and forward to the Demobilization unit. The Demobilization Unit will compile a tentative list of surplus resources from these lists from all Command and General Staff and submit a consolidated release list to the Incident Commander/Unified Command for approval (via the Planning Section Chief). This form can be accessed directly at: https://media.defense.gov/2017/Jul/28/2001784777/-1/-1/0/ICS_236_CG.PDF.

Role-Specific Documentation

In addition to the ICS Forms, different ICS functional areas and roles rely on a variety of other types of documentation to perform their responsibilities. These other types of documentation are listed below, organized by functional areas.

Command/Administration:

- Agency Administrator Briefing Packet
- Delegation of Authority (DOA)/Return of DOA
- Disciplinary/Sensitive Items
- Incident Narrative/Executive Summary
- ICS Organization Transition/Debriefing
- Incident Complexity Analysis
- Significant Events Narratives/Reports
- Special Interest/Political Inquiries

Human Resources (HR):

- Critical Incident Stress Management Narratives
- HR Significant Event Reports

Public Information:

- Community Relations/Public Service Announcements (PSAs)
- Closure Orders/Restrictions
- Information Summary/Communications Strategy
- Media Log/Key Contacts/Traplines/Public Phone Call Log
- Media Releases/Daily Incident Updates
- Newspaper Clippings
- Public Meeting Agendas/Notes/Briefings
- Special Events/Tours/Very Important Person (VIP) Visits
- Thank You Letters
- Web Pages/Videos/Photos/Blogs/Interactive Maps/Dashboards
- Social Media Posts

Liaison/Agency Representation:

- Contact Logs/Conversation Records
- Liaison Officer Significant Events/Reports

Safety:

- Accident Investigation Reports
- Hazard Abatement/Safety Strategy
- Job Hazard Analysis (JHA)
- Safety Inspections/OSHA Reports
- SAFENETs

Operations Section:

- Contingency Plans
- Demobilization Glide Path
- Evacuation/Re-Entry Plans
- Strategies/Tactics
- Structure Defense/Protection Plan(s)

Operations Section/Air Operations:

- Aircraft Authorizations
- Flight Use/Hour Tracking Documentation
- Helibase Daily Use/Cost Summary
- Miscellaneous Helibase Documentation

Planning Section:

- Photos (with captions)

Planning Section/IT Support:

- Equipment/Property Records
- Demobilization Unit:
- Demobilization Plan
- Final Resources Database Printout
- Performance Evaluations (OH, Crews, Equipment)
- Rest and Relaxation (R&R) Plan/Information

Planning Section/Documentation Unit:

- Master Documentation Index

Planning Section/Resources Unit:

- Resource Tracking Glide Path
- Resource Advisor Information/Plans
- Suppression Repair/Rehabilitation Plan

Planning Section/Situation Unit:

- Agency Jurisdiction/Ownership Map
- Incident Perimeter Maps
- Incident Progression Maps
- Geospatial Information System (GIS) Data
- Infrared Imagery (with interpretation)
- Maps – Special Products (not daily operations)
- Structural Damage Assessments
- Technical Specialist Function Areas:
- Incident Narrative Technical Reports/Final Report
- Daily Technical Reports
- Contingency Plans

Logistics Section/Communications Unit:

- Communications Equipment Inventories
- Radio Traffic Logs/Telephone Logs
- Repeater Site Documentation
- Radio Repairs
- Logistics Section Facilities Unit:
- Facilities Health Inspections
- Land Use Agreement Information

Logistics Section/Food Unit:

- Caterer – Menu/Meal Logs
- Caterer – Orders/Waybills
- Food/Caterer Health Inspections

Logistics Section/Ground Support Unit:

- Equipment Repair Orders
- Hazard Mitigation – Noxious Weeds/Hazardous Materials Documentation
- Optional Form (OF) 296 Vehicle/Heavy Equipment Inspection Checklists
- Rental Vehicle Checkout List and Inventory
- Vehicle Dispatch Logs (for Buses, Pick-ups, etc.)

Logistics Section/Medical Units:

- Accident Action Plan
- Medical Injury/Treatment Logs
- Medical Issue Logs
- Patient Medical Evaluations

Logistics Section/Security Unit:

- Patrol Logs
- Security Plan
- Logistics Section Supply Unit:
- Accountable Property Summary to Cache
- Incident Replacement Authorizations
- Cache Issue Report
- Daily Inventories
- Property Issue Logs
- Property Loss/Salvage Reports
- Saw Parts Orders
- Supply Issue Logs
- Waybills/Buying Team Waybills

Finance Section/Compensation/Claims Unit:

- Comp for Injury Documents/Logs
- Property Damage Claims/Logs

Finance Section/Cost Unit:

- Aircraft Costs – Rotary/Fixed Wing
- Cost Share Apportionment/Agreements
- Cost Summary (Cumulative)
- Cost Management
- Final Statement of Costs
- Final Daily Cost Tracking Database Printouts

Finance Section/Procurement Unit:

- Buying Team Purchase Receipts
- Buying Team Purchase Logs/Equipment Logs
- Commissary – Contract/Costs/Claims
- Contract Letter to Contracting Officer
- Contractor Performance Evaluations
- Emergency Equipment Rental Agreements (EERA)
- Equipment Time/Records/Claims
- Invoices/Issue Reports
- Operating Plans
- Pricing Issues

Finance Section/Time Unit:

- Excessive Shift Justifications
- I-9s and Tax Forms
- Length of Assignment Extensions
- Personnel Time Records
- Work/Rest Justification Worksheets

ICS Forms Responsibility and Distribution

ICS Forms	Title	IAP Component	Section Responsible	Originator	Approvals Required	Distribution
201	Incident Briefing	No	Command	Initial Action Incident Commander	None	Situation and Resources Units
202	Incident Objective	Yes	Planning	Planning Section Chief	Incident Commander	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders
203	Organization Assignment List	Yes	Planning	Resources Unit	None	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders
204	Assignment List	Yes	Planning	Resources Unit	Planning Section Chief	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders
205	Incident Radio Communications Plan	Yes	Logistics	Communications Unit Leader	None	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders
205A	Communications List	Optional	Logistics	Communications Unit Leader	None	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders
206	Medical Plan	Yes	Logistics	Medical Unit Leader	Safety Officer	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders
207	Incident Organization Chart	No	Planning	Resources Unit	None	Command Post Display
208	Safety Message/Plan	Yes	Command	Safety Officer	None	Planning Meeting Prop

ICS Forms	Title	IAP Component	Section Responsible	Originator	Approvals Required	Distribution
209	Incident Status Summary	No	Planning	Situation Unit	Planning Section	Command Staff, General Staff, Unit Leaders Dispatch Center, ICP Display
210	Resource Status Change	No	Logistics	Incident Communication Center Manager – to record status change received from incident personnel	None	Communications Unit. Resources Unit T-Card Display
211	Incident Check-in List	No	Planning	Communication Center, Resources Unit, Staging Area, Incident Base, Camp, and Helibase	None	Resources Unit and Finance Section
212	Incident Demobilization Vehicle Safety Inspection	No	Logistics	Ground Support Unit	Inspector	Vehicle Operator, Incident File
213	General Message	No	ALL	Communications Center or any Message Originator	None	Original to Addressee
214	Activity Log	Occasionally a blank is ICS Form 214 the last page in the IAP	ALL	Section Chiefs, Branch Directors, Division/Group Supervisors, Unit and Strike Team/Resource Team Leaders	None	Immediate Supervisor
215	Operational Planning Worksheet	No	Operations and Planning	Operations Chief, Resources Unit Leader	Incident Commander (at the Planning Meeting)	Planning Meeting Prop

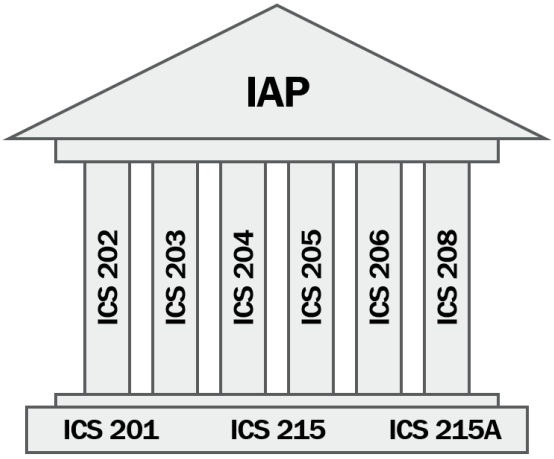
ICS Forms	Title	IAP Component	Section Responsible	Originator	Approvals Required	Distribution
215-A	Incident Action Safety Plan Analysis	No	Safety Officer	Safety Officer	Incident Commander (at the Planning Meeting)	Planning Meeting Prop
216	Radio Requirements Worksheet	No	Logistics	Communication Unit	None	Internal Communication Unit Worksheet
217	Radio Frequency Assignment Worksheet	No	Logistics	Communications Unit	None	Internal Communication Unit Worksheet
218	Support Vehicle Inventory	No	Logistics	Ground Support Unit	None	Resources Unit
219	Resource Status Card (1-10)	No	Planning	Resources Unit	None	Posted in Resources Unit T-Card Display
220	Air Operations Summary Worksheet	Where Applicable	Operations	Air Operation Branch Director	None	All Section Chiefs, Branch Directors, Division/Group Supervisors, and Unit Leaders, ICP Display
221	Demobilization Check-out	No	Planning	Demobilization Unit	None	Incident File
222	Incident Weather Forecast Request	No	Planning	Situation Status Unit	None	Incident File
223	Tentative Release List	Occasionally	Planning	Demobilization Unit Leader	Section Chief	Possibly in the IAP, Display on the Information Boards
224	Crew Performance Rating	No	All	Supervisors	None	Incident File, Home Unit
225	Incident Personnel Performance Rating	No	All	Supervisors	None	Incident File, Home Unit

ICS Forms	Title	IAP Component	Section Responsible	Originator	Approvals Required	Distribution
226	Compensation for Injury Log	No	Finance Admin	Compensation Claims Log	None	Internal Compensation Unit Worksheet
227	Claims Log	No	Finance Admin	Compensation Claims Unit	None	Incident File
228	Incident Cost Worksheet	No	Finance Admin	Cost Unit	None	Incident File
229	Incident Cost Work Summary	No	Finance Admin	Cost Unit	None	Incident File

Appendix E: SAMPLE IAP

This section includes a completed IAP using the Fairground scenario. Note that an IAP may have several form 204s.

Figure 55: IAP Components

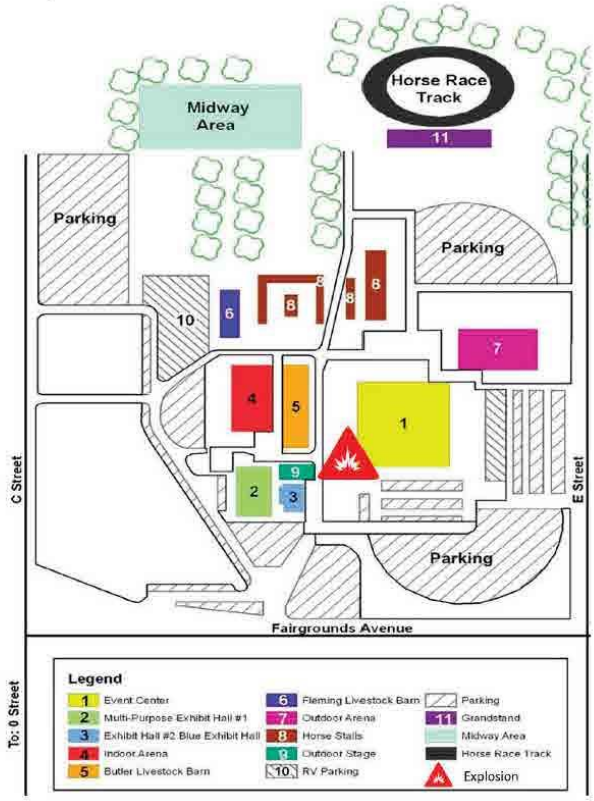


INCIDENT BRIEFING (ICS 201)

1. Incident Name:	2. Incident Number:	3. Date/Time Initiated:
Liberty County Fairgrounds		Date: 08/15/20xx Time: 2015

4. Map/Sketch (include sketch, showing the total area of operations, the incident site/area, impacted and threatened areas, overflight results, trajectories, impacted shorelines, or other graphics depicting situational status and resource assignment):

See Fairgrounds Explosion Map



5. Situation Summary and Health and Safety Briefing (for briefings or transfer of command): Recognize potential incident Health and Safety Hazards and develop necessary measures (remove hazard, provide personal protective equipment, warn people of the hazard) to protect responders from those hazards.

Report is 15 mins after the incident began. The Central City Fire Department has established Incident Command. Public safety personnel on scene: law enforcement, fire, and EMS responded immediately to the incident. Single resources include: fire trucks, ambulances, and law enforcement officers.
Initial identified hazards included:
The propane explosion with the potential to spread to structures.
Potential hazardous material release from other facilities.
Potential for explosions if the fire encounters fuel or compressed gas cylinders.
Potential structural collapse of the building due to the explosion.
The safety concerns include:
Harm to civilians or emergency responders due to the aforementioned hazards.
Injured people are unable to self-evacuate from the immediate area of the fire.

6. Prepared by: Name: _____ Position/Title: _____ Signature: _____

ICS 201, Page 1 Date/Time: _____

INCIDENT BRIEFING (ICS 201)

1. Incident Name:	2. Incident Number:	3. Date/Time Initiated:
Liberty County Fairgrounds		Date: 08/15/20xx Time: 2015

7. Current and Planned Objectives:

Evacuate all injured personnel from the vicinity of the explosion to the on-scene medical personnel timely and efficiently.
Provide on-site triage, stabilization, and hospital transport for victims within timely and efficiently.
Extinguish vehicle fire timely and efficiently.
Mitigate leaks of flammable fuels and compressed gas to prevent expansion of the fire within 2 hours (by 2215)
Establish a controlled perimeter around the incident within 45 minutes (by 2100)
Manage traffic on Fairgrounds Avenue, C Street, and E Street to ensure responder access within 30 minutes (by 2045)

8. Current and Planned Actions, Strategies, and Tactics:

Time:	Actions:
2045	Push out public messages for citizens to stay out of the area, more information will be provided asap.
2100	Ensure all onsite resources are accounted for and documented with estimated start time.
2200	Ensure IMT has full access to the CP location and initial supplies to include comms, event maps, & plans.

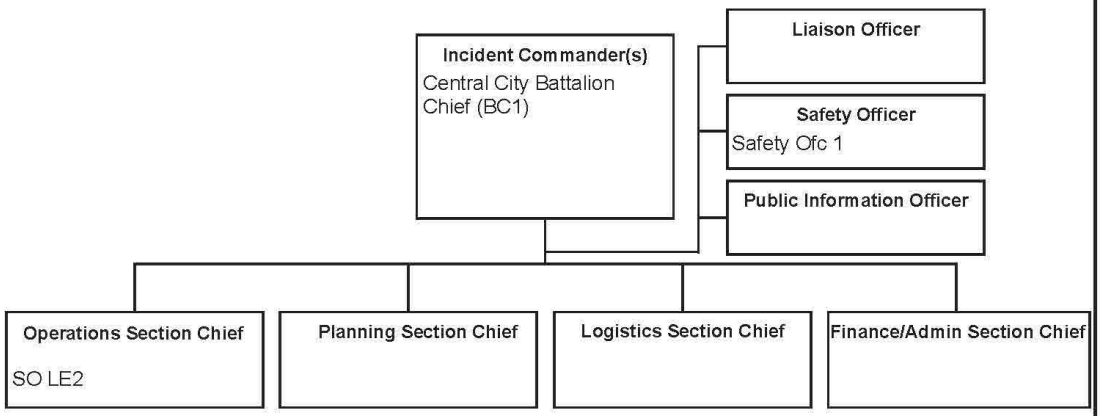
6. Prepared by: Name: _____ Position/Title: _____ Signature: _____

ICS 201, Page 2 Date/Time: _____

INCIDENT BRIEFING (ICS 201)

1. Incident Name:	2. Incident Number:	3. Date/Time Initiated:
Liberty County Fairgrounds		Date: 08/15/20xx Time: 2015

9. Current Organization (fill in additional organization as appropriate):



6. Prepared by: Name: _____ Position/Title: _____ Signature: _____

ICS 201, Page 3 Date/Time: _____

INCIDENT BRIEFING (ICS 201)

1. Incident Name: Liberty County Fairgrounds	2. Incident Number:	3. Date/Time Initiated: Date: 08/15/20xx Time: 2015

10. Resource Summary:

Resource	Resource Identifier	Date/Time Ordered	ETA	Arrived	Notes (location/assignment/status)
Staffed fire apparatus	CCE1	8/15/xx 2005		☒	Crew of 4, fire suppresion, onsite mitigating the engulfed main hall structure
Staffed fire apparatus	CCT1	8/15/xx 2005		☒	Crew of 4, fire suppression, onsite mitigating engulfed livestock barn
Ambulance (ALS)	EMS1	8/15/xx 2005		☒	Crew of 2, one ambulance, onsite supporting TTT team with transport
Ambulance (ALS)	EMS2	8/15/xx 2005		☒	Crew of 2, one ambulance, onsite supporting TTT team with treatment
Law enforcement for traffic control	CC Badge#	8/15/xx 2005		☒	10 officers, onsite reporting to one Sgt. moving them as needed, contact Sgt for info.
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	
				☐	

6. Prepared by: Name: _____ Position/Title: _____ Signature: _____

ICS 201, Page 4 Date/Time: _____

OPERATIONAL PLANNING WORKSHEET (ICS 215)

1. Incident Name: Liberty County Fairgrounds Incident

2. Operational Period: Date From: 8/16/XX Time From: 0700 Date To: 8/17/XX Time To: 0700

3. Branch	4. Division, Group, or Other	5. Work Assignment & Special Instructions	6. Resources	2-person uniformed [redacted]	Hazmat	PWST	LE Investigative TF	Engine	Ambulance (2 ALS)	USAR TF	Reunification Personnel	Shelter Personnel				7. Overhead Position(s)	8. Special Equipment & Supplies	9. Reporting Location	10. Requested Arrival Time
	LE	Perimeter and traffic control	Req.	24													Traffic Control Supplies	Onscene	Immediate
			Have	20															
			Need	4															
	Hazmat	Mitigate Hazards	Req.		16												Hazmat gear	Onscene	Immediate
			Have		16														
			Need																
	DA	Structural Damage Assessment	Req.			6											Damages Reports	Onscene	Immediate
			Have			4													
			Need			2													
	Investigations	Criminal Investigation	Req.				8										Drone	Onscene	Immediate
			Have				6												
			Need				2												
	Exting	Extinguish fire and complete cleanup	Req.					4										Onscene	Immediate
			Have					4											
			Need																
	EMS	Treatment and Transport	Req.						4								ALS (2)	Onscene	Immediate
			Have						4										
			Need																
		11. Total Resources Required		24	16	6	8	4	4										
		12. Total Resources Have on Hand		20	16	4	6	4	4										
		13. Total Resources Need To Order		4		2	2												

14. Prepared by:
Name: Marilyn Gibson
Position/Title: OSC
Signature:
Date/Time: 8/16/XX 0500

ICS 215

OPERATIONAL PLANNING WORKSHEET (ICS 215)

1. Incident Name: Liberty County Fairgrounds Incident

2. Operational Period: Date From: 8/16/XX Time From: 0700 Date To: 8/17/XX Time To: 0700

3. Branch	4. Division, Group, or Other	5. Work Assignment & Special Instructions	6. Resources	2-person uniformed [redacted]	Hazmat	PWST	LE Investigative TF	Engine	Ambulance (2 ALS)	USAR TF	Reunification Personnel	Shelter Personnel				7. Overhead Position(s)	8. Special Equipment & Supplies	9. Reporting Location	10. Requested Arrival Time
	USAR	Search and Rescue	Req.							8							PPE for rubble/debris	Onscene	Immediate
			Have							4									
			Need							4									
	Reunification	Staff Reunification center and manage tracking	Req.								8							Reunification Center	Immediate
			Have								6								
			Need								2								
	Shelter	Staff shelter locations	Req.									10						Shelter locations	Immediate
			Have									5							
			Need									5							
			Req.																
			Have																
			Need																
			Req.																
			Have																
			Need																
			Req.																
			Have																
			Need																
		11. Total Resources Required								8	8	10					**14. Prepared by:** Name: Marilyn Gibson		
		12. Total Resources Have on Hand								4	6	5					Position/Title: OSC		
		13. Total Resources Need To Order								4	2	5					Signature: Date/Time: 8/16/XX 0500		

ICS 215

INCIDENT ACTION PLAN SAFETY ANALYSIS (ICS 215A)

1. Incident Name: Liberty County Fairgrounds Incident		2. Incident Number:
3. Date/Time Prepared: Date: 8/16/XX Time: 0500	4. Operational Period: Date From: 8/16/XX Time From: 0700	Date To: 8/17/XX Time To: 0700

5. Incident Area	6. Hazards/Risks	7. Mitigations
LE- Perimeter and traffic control	Traffic, night conditions, weather, physical health	Personal and emergency lighting, reflective gear, water, appropriate breaks and rest time.
Hazmat- Mitigate Hazards	Hazardous material, night conditions, weather, physical health	PPE, hazmat protocol, water, appropriate breaks and rest time.
DA- Structural damage assessment	Weather, debris, structural stability, physical health	ACT-20 Rapid Assessment, PPE, water, appropriate breaks and rest time.
Investigations- Criminal investigation	Weather, hazmat area, debris, physical health	PPE, be aware of potential hazardous materials and/or debris in the area, appropriate breaks and rest time.
Exting- Extinguish fire and complete	Fire, hazmat, debris, physical health, weather	PPE, hazmat protocol, water, appropriate breaks and rest time
EMS- Treatment and Transport	Weather, hazmat area, debris, physical health	PPE, be aware of potential hazardous materials and/or debris in the area, appropriate breaks and rest time
Rescue	Weather, hazmat, debris, physical health, structural stability	PPE, be aware of potential hazardous materials and/or debris in the area, appropriate breaks and rest time.
Reunification- Staff Reunification	Utility outages, physical health	Backup generators for lighting, AC; appropriate breaks and rest time.
Shelter- Staff shelter locations	Utility outages, physical health	Backup generators for lighting, AC; appropriate breaks and rest time.

8. Prepared by (Safety Officer): Name: Grady Potts	Signature:
Prepared by (Operations Section Chief): Name: Marilyn Gibson	Signature:
ICS 215A	Date/Time: 8/16/XX 0500

INCIDENT OBJECTIVES (ICS 202)

1. Incident Name: Liberty County Fairgrou	2. Operational Period: Date From: 08/16/XX Date To: 08/17/XX Time From: 0700 Time To: 0700

3. Objective(s):

1. Law Enforcement Perimeter Group to provide safety and security of the fairground footprint by staffing the perimeter with uniformed officers and coordinating access of ingress/egress points.
2. Law Enforcement Investigations Group to continue to process and support investigation of the scene and related follow-up.
3. Law Enforcement Traffic Control Group to staff identified traffic control positions with uniformed officers to safely route vehicle traffic around the incident and through the highly congested area of impact.
4. Reunification team to cross-reference reports of missing, injured, and deceased persons with information reported at the reunification center/shelter, via the reunification hotline, reunification posts on social media, and emergency dispatch with the on-hand tracking sheet and the identified hospital patient tracking contact. Provide loved ones with timely and accurate information as soon as available and follow all hospital protocols when sharing information about those currently under their care. Any on-scene death notices will be handled by the Liberty County Coroner's Office.
5. Support and coordinate shelter supplies, resources, and physical and/or mental health needs for those impacted by the incident.
6. EMS continue to provide support of the on-scene search and rescue operations and first responders as needed.
7. Hazmat teams to continue work on the removal of fuel and other materials from the fairground site and monitor the surrounding fairground area for any fires or hazmat concerns.
8. Rescue Team focus search and rescue efforts in and around the Event Hall and surrounding buildings.
9. Damage Assessment team to provide initial reports of all structure damages and then follow up with complete report when the area/structure is safe to do so.

4. Operational Period Command Emphasis:

Ongoing operations continue within the fairgrounds. The surrounding area continues to be impacted by the aftermath of the incident. Stay vigilant, monitor activities in the area, support where possible, but remain within the scope set by the listed objectives.

General Situational Awareness

There are ongoing hazards in the incident area to include HazMat and LE investigations. The local area is currently experiencing power and gas outages, traffic disruptions, and high temperatures that may cause concerns for residents to remain safely in their homes. The emergency shelter continues to operate to support those who were evacuated.

5. Site Safety Plan Required? Yes ☒ No ☐

Approved Site Safety Plan(s) Located at: Plans/HazMat Group

6. Incident Action Plan (the items checked below are included in this Incident Action Plan)**:**

☒ ICS 203	☒ ICS 207	Other Attachments:
☒ ICS 204	☒ ICS 208	☐ _____
☒ ICS 205	☒ Map/Chart	☐ _____
☒ ICS 205A	☒ Weather Forecast/Tides/Currents	☐ _____
☒ ICS 206		☐ _____

7. Prepared by: Name: Amani Cruz Position/Title: PSC Signature: _____

8. Approved by Incident Commander: Name: Pablo McClain Signature: _____

ICS 202	IAP Page _____	Date/Time: 8/16/XX 0500

ORGANIZATION ASSIGNMENT LIST (ICS 203)

1. Incident Name:	2. Operational Period: Date From: 08/16/XX Date To: 08/17/XX
Liberty County Fairgrounds Incident	Time From: 0700 Time To: 0700

3. Incident Commander(s) and Command Staff:	
IC/UCs	Pablo McClain
	Liberty County Sheriff Kash Goodman
Deputy	
Safety Officer	Grady Potts
Public Info. Officer	Aidyn Walters
Liaison Officer	Kaylyn Mercer

4. Agency/Organization Representatives:	
Agency/Organization	Name
Liberty County Manager	John Dulay
Central City Mayor	Robert Cassiday
Central City EMS Chief	John Howard
Central City Water Superir	Lynwood O'Neal

5. Planning Section:	
Chief	Amani Cruz
Deputy	
Resources Unit	Ruby Macias
Situation Unit	Manny Horowitz
Documentation Unit	
Demobilization Unit	
Technical Specialists	

6. Logistics Section:	
Chief	Magdalena Tanner
Deputy	
Support Branch	
Director	
Supply Unit	
Facilities Unit	
Ground Support Unit	
Service Branch	
Director	
Communications Unit	Destiney Sexton
Medical Unit	Kaycee Lairson
Food Unit	

7. Operations Section:		
Chief	Marilyn Gibson	
Deputy		
Staging Area		
Branch		
Branch Director		
Deputy		
Division/Group	Perimeter	LE 3
Division/Group	Traffic Control	LE 3
Division/Group	Investigations	LE 4
Division/Group		
Division/Group		
Branch		
Branch Director		
Deputy		
Division/Group	HazMat	FD 5
Division/Group	Damage Assessment	PW 1
Division/Group	Extinguishment	FD 3
Division/Group	EMS	EMS 1
Division/Group	Rescue Team	R 1
Branch		
Branch Director		
Deputy		
Division/Group	Reunification	RU 1
Division/Group	Shelter	S 1
Division/Group		
Division/Group		
Division/Group		
Division/Group		
Air Operations Branch		
Air Ops Branch Dir.		

8. Finance/Administration Section:	
Chief	Paloma Andrews
Deputy	
Time Unit	
Procurement Unit	
Comp/Claims Unit	
Cost Unit	

9. Prepared by: Name: Amani Cruz Position/Title: PSC Signature: _____

ICS 203 | **IAP Page** _____ Date/Time: 08/16/XX 0500

ASSIGNMENT LIST (ICS 204)

1. Incident Name:	2. Operational Period:		3.
Liberty County Fairgrounds Incident	Date From: 08/16/XX	Date To: 08/17/XX	**Branch:**
	Time From: 0700	Time To: 0700	**Division:**

4. Operations Personnel: Name — Contact Number(s)

Operations Section Chief: Marilyn Gibson

Branch Director:

Division/Group Supervisor: FD 5

Group: HazMat

Staging Area: Station 4

5. Resources Assigned:

Resource Identifier	Leader	# of Persons	Contact (e.g., phone, pager, radio frequency, etc.)	Reporting Location, Special Equipment and Supplies, Remarks, Notes, Information
HazMat 1	HM 1	6	Radio Channel	Report to staging area
HazMat 2	HM 2	6	Radio Channel	Report to staging area
HazMat 3	HM 3	6	Radio Channel	Report to staging area

6. Work Assignments:

Three HazMat teams comprised of 1 leader and 6 personnel. Complete review of identified Hazardous materials in the incident and mitigate the hazards to allow ongoing first responder operations.

7. Special Instructions:

Use HazMat protocol and ensure all personnel are using appropriate PPE. Report any injuries immediately via chain of command.

8. Communications (radio and/or phone contact numbers needed for this assignment)**:**

Name/Function	Primary Contact: indicate cell, pager, or radio (frequency/system/channel)
FD 5 /	Radio
/	
/	
/	

9. Prepared by: Name: Marilyn Gibson Position/Title: OSC Signature:

ICS 204 | **IAP Page** ____ Date/Time: 8/16/XX 0500

INCIDENT RADIO COMMUNICATIONS PLAN (ICS 205)

1. Incident Name:	2. Date/Time Prepared:	3. Operational Period:
Liberty County Fairgrounds Incident	Date: 08/16/XX 0200 Time:	Date From: 08/16/XX Date To: 08/17/XX Time From: 0700 Time To: 0600

4. Basic Radio Channel Use:

Zone Grp.	Ch #	Function	Channel Name/Trunked Radio System Talkgroup	Assignment	RX Freq N or W	RX Tone/NAC	TX Freq N or W	TX Tone/NAC	Mode (A, D, or M)	Remarks
	1	Command		Command	154.900 N		154.385 N	156.7	D	Monitored by Liberty County Dispatch
	2	Tactical		Perimeter	155.040 N		155.040 N	156.7	D	
	3	Tactical		Traffic Control	488.912 W		488.912 W	D162	D	
	4	Tactical		Investigations	460.575 N		460.575 N	162.2	A	
	5	Tactical		Extinguishment	160.050 N		160.050 N	156.7	D	
	6	Tactical		Rescue / USAR	155.652 N		155.652 N	136.5	D	
	7	Tactical		HazMat	156.574 N		156.574 N	156.7	D	
	8	Support		EMS	169.900 FM		169.900 FM			

5. Special Instructions:

6. Prepared by (Communications Unit Leader): Name: Destiney Sexton Signature: _____

ICS 205	IAP Page _____	Date/Time: 08/16/XX 0500

COMMUNICATIONS LIST (ICS 205A)

1. Incident Name: Liberty County Fairgrounds Incident	2. Operational Period: Date From: 8/16/20XX Time From: 0700	Date To: 8/17/20XX Time To: 0700

3. Basic Local Communications Information:

Incident Assigned Position	Name (Alphabetized)	Method(s) of Contact (phone, pager, cell, etc.)
Central City Mayor	Robert Cassiday	200-555-1971
Liberty International Airport Mgr	Catron, M	555-0044
Communications Unit Leader	Destiney Sexton	555-6172
Liberty County Manager	John Dulay	555-9870
EMS Group	EMS 1	555-6767
Planning Section Chief	Amani Cruz	555-8763
Extinguishment Group Superviso	FD 3	555-6177
HazMat Group	FD 5	555-6784
Incident Commander	Pablo McClain	200-555-1212
EMS Director	Chief Dr John Howard	555-6171
Operations Section Chief	Marilyn Gibson	555-4455
LE Division Supervisor	LE 3	555-0985
Investigations Supervisor	LE 4	555-9879
Liaison Officer	Kaylyn Mercer	555-9841
Logistics Section Chief	Magdalena Tanner	555-6196
Central City Superintendent	Michael A Martinez	555-8745
Medical Unit Leader	Kaycee Lairson	555-9874
Finance Section Chief	Paloma Andrews	555-121-1234
Public Information Officer (PIO)	Aidyn Walters	200-555-1200
Damage Assessment	PW1	555-0984
Reunification Group	RU 1	555-1212
Safety Officer	Grady Potts	555-0987
Incident Commander	Jeff Shrader	555-4093
Red Cross Rep.	Marilyn Jefferson	555-5646
Shelter Division	S 1	555-6170
Time Unit Leader	Lola Cantrell	555-0900
Branch Director	US 1	555-8751
Veterinary Services Group	Vet 1	555-7112
Resource Unit Leader	Ruby Macias	555-0123
Supply Unit Leader	Kaylie Underwood	555-9352
		555-5673

4. Prepared by: Name: Destiney Sexton	Position/Title: COML	Signature:
ICS 205A | IAP Page _____	Date/Time: 5/21/20XX 1600	

MEDICAL PLAN (ICS 206)

1. Incident Name:	2. Operational Period:			
Liberty County Fairgrounds Incident	Date From: 08/16/XX	Time From: 0700	Date To: 08/17/XX	Time To: 0700

3. Medical Aid Stations:

Name	Location	Contact Number(s)/Frequency	Paramedics on Site?
Incident Aid Station #1	JJ & 7th St	EMS Channel	☒ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

4. Transportation (indicate air or ground)**:**

Ambulance Service	Location	Contact Number(s)/Frequency	Level of Service
Med Flight 1	Capital City Hospital	xxx-xxx-xxxx	☒ ALS ☐ BLS
Bayport Ambulance Service	Ferry Blvd & 7th Ave, Bayport	xxx-xxx-xxxx	☒ ALS ☐ BLS
Fisherville Ambulance	F & 7th St, Fisherville	xxx-xxx-xxxx	☐ ALS ☒ BLS
Central City EMS	W & 12th St	xxx-xxx-xxxx	☒ ALS ☐ BLS

5. Hospitals:

Hospital Name	Address, Latitude & Longitude if Helipad	Contact Number(s)/ Frequency	Travel Time		Trauma Center	Burn Center	Helipad
			Air	Ground			
Harvest Junc Community	C & 23rd St Harvest Junction	xxx-xxx-xxxx		7 min	☒ Yes Level: III	☐ Yes ☒ No	☐ Yes ☒ No
Kingston Region Medical Facility	P & 18th St Kingston	xxx-xxx-xxxx	5 min	10 min	☒ Yes Level: III	☐ Yes ☒ No	☒ Yes ☐ No
Noble General Hospital	S & 1st St Fisherville	xxx-xxx-xxxx	7 min	14 min	☒ Yes Level: III	☐ Yes ☒ No	☒ Yes ☐ No
Grand County Hospital	North Castle Metropolis	xxx-xxx-xxxx	30 min	75 min	☒ Yes Level: I	☒ Yes ☐ No	☒ Yes ☐ No
					☐ Yes Level:	☐ Yes ☐ No	☐ Yes ☐ No

6. Special Medical Emergency Procedures:

Notify Supervisor of any Injury/Medical Emergency. Supervisors will ensure EMS has been notified on Command Channel for treatment and notify C-O-C and SOFR. Info needed: type of injury, mechanism, type of transport needed, and location.
Incident Aid Station 1 can be used for minor injuries.
Supervisor complete proper injury/medical forms.

☐ Check box if aviation assets are utilized for rescue. If assets are used, coordinate with Air Operations.

7. Prepared by (Medical Unit Leader)**:** Name: Kaycee Lairson Signature: _____

8. Approved by (Safety Officer)**:** Name: Grady Potts Signature: _____

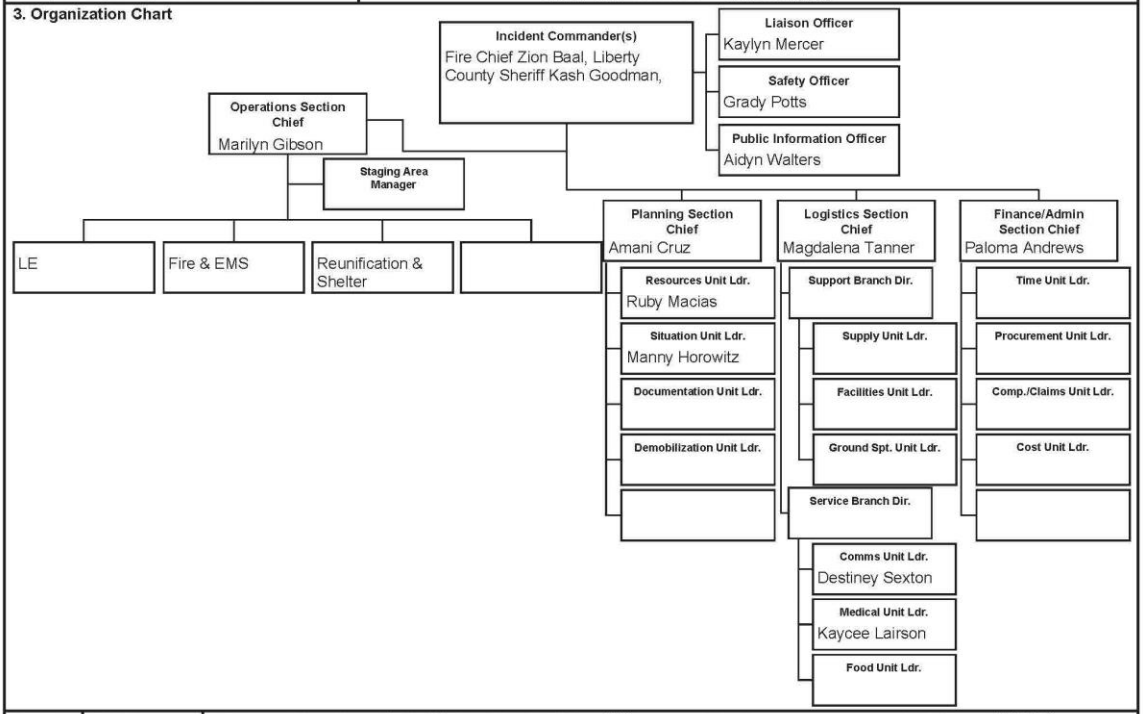
ICS 206 | **IAP Page** _____ | Date/Time: 08/16/XX 0500

INCIDENT ORGANIZATION CHART (ICS 207)

1. Incident Name: Liberty County Fairgrounds Incident

2. Operational Period: Date From: 08/16/XX Date To: 0700 Time From: 08/17/XX Time To: 0700

3. Organization Chart



ICS 207 | **IAP Page** ___ | **4. Prepared by:** Name: Amani Cruz Position/Title: PSC Signature: _____ Date/Time: 08/16/XX

SAFETY MESSAGE/PLAN (ICS 208)

1. Incident Name:	2. Operational Period: Date From: 08/16/XX Date To: 08/17/XX Time From: 0700 Time To: 0700
Liberty County Fairgrounds Incident	

3. Safety Message/Expanded Safety Message, Safety Plan, Site Safety Plan:

SAFETY IS EVERYONE'S JOB, MAKE IT YOUR PRIORITY!

Correct and confront unsafe conditions:
- Wear appropriate/approved PPE for work assignments/tasks
- Use caution in and around structures as they may be unstable and are a collapse potential
- Be mindful in working around debris with sharp edges that can cut
- Avoid and mitigate slip, trip, and fall hazards
- Use proper lifting techniques

Monitor work rest ratios by taking breaks as needed to reduce fatigue

Drink plenty of fluids to maintain level of hydration

Be mindful of potential hazards from downed utility wires - treat all as energized

Maintain situational awareness around moving traffic

Wear high visibility traffic vests when assigned to work in areas of traffic movement

Immediately report injuries and/or accidents to your supervisor and to the Safety Officer

Review ICS-206 Medical Plan to familiarize yourself with medical aid stations and protocol to request and receive medical assistance

4. Site Safety Plan Required? Yes ☒ No ☐ Plans / HazMat group

Approved Site Safety Plan(s) Located At:

5. Prepared by: Name: Grady Potts Position/Title: Safety Officer Signature: _____

ICS 208	IAP Page _____	Date/Time: 08/16/XX 0500

Appendix F: Incident Management Teams by Thomas E. Tarp

California Department of Forestry and Fire Protection

Editor's Note: In the fall of 2021, a team of subject matter experts, along with the primary author, came together to update original article that has been part of the National Incident Management System (NIMS) Incident Command System (ICS) position training since its inception. The team's focus was to update the content to be more contemporary, aligning it with current practices, changes in language and terminology. The second task was to link key concepts, thoughts and applications to the material presented throughout the *Incident Command System (ICS) Position Training Foundations Course Reference Guide (Reference Guide)* as examples for students taking part in position specific training. The core of the article is intact.

Preface – By the original primary author – Chief Thomas Tarp

The following article has a unique history and purpose. This product is a portion of a much larger product which was originally developed by Command Teams 4 and 6 of California Department of Forestry and Fire Protection during the early 1990s.

The writing team's development method consisted of ideas and concepts being bullet-pointed and sent to Command and General Staff members for review and input. These were then compiled and edited into what you see. These gems of experience, which are from a wide variety and number of complex emergencies by actual team members, are presented for your consideration and/or application.

Due to article length, some portions of the entire transcript are not included. Reasons for this vary. Some content was specific to organized California Department of Forestry and Fire Protection Command/Management Teams and not considered necessary for this training process. Some content was outdated without current application. The intent is for you view this information and to afford you some "words of wisdom" from experienced/knowledgeable folks.

A word of **Caution**- The experience/information presented is not to be construed as the only possible solution to situations as they arise during assignments. Rather, information shows the wide variety of impacts that have been encountered by the writers and presents suggested remedies from their experiences. Consider, as you encounter new and unknown situations, that the application of this information may serve as an aid to you in determining your approach to an incident.

It is nearly certain that you will encounter new situations and unexpected impacts will happen. Not all will be within the "normal" box, nor will they be listed in any textbook. You

must address these situations. They will require creative thinking, will test your decision-making, and must be handled professionally.

This document was originally developed to orient new members to a command team setting by outlining general operating procedures. An unintended benefit of this document has been the use of it in training.

A final note before we get into the article; capturing experience-based tidbits often is not done well. As you gain experience in the profession of emergency response, consider how you might continue this effort and allow others to gain valuable insights from your experiences.

Section 1 - An Introduction to Lessons Learned

CONGRATULATIONS! You have been selected to be a member of an Incident Management Team (IMT). This could be a new assignment, or you could be a seasoned veteran. Regardless, to be so selected you must have showed that you have the knowledge, experience and leadership needed to manage complex emergencies. For many, this will be considered the pinnacle of their fire service or resource management career.

What you probably were not told about this appointment was some unique associated roles coming your way. Simultaneously, during an actual emergency, you may be considered a hero and a villain, an emergency management expert and a great waste of taxpayer money, a savior to some and a dunderhead to others. You may also assume the positions of dictator, saint, reverend, executive, grand inquisitor, teacher, student, leader, follower, drill sergeant, politician, mother, or father, as well as many others. Throw in very long work hours, more than just a little stress accompanied by too much caffeine, and it is a wonder you don't lock-up both mentally and physically. But you won't. Besides, it's not good for the image.

There are two other things this appointment brings, expectations that are implied and may not have been explained to you. First, that you will apply your training, knowledge, and experience to the best of your abilities while performing within the team setting. Second, that you will aid in the development of others met during a deployment so that one day they, too, can assume greater responsibilities as you have. To meet these expectations, just give an honest shot of your best and you will be surprised with the positive results.

There will be times when you will be blazing new trails in disaster and incident response both for yourself and your team. There is also the chance it will be a new trial for your agency. Not much pressure, right?

Whenever an individual is faced with new and difficult challenges, some "experts" say we mentally revert to a past situation that comes close to mirroring our current problem and we base decisions and actions on that experience. We all have stored memories that we draw upon. When confronted with a new challenge, we mentally hurry through our memory logs looking for a situation that comes close to what is in front of us and pull successful actions

from those logs to assimilate whatever we are facing. As you face new challenges while on your Incident Management Team (IMT) assignments, you will be tapping into your own experiences continually.

Is your personal inventory of experiences current and full? One purpose of this essay is to add some tips, experiences, and best practices-based on the experiences of past IMTs that you can add to your inventory. It is doubtful that any "textbook" answers will be provided; in fact, that won't even be tried. And for very good reason.

Just as each emergency is different in the demands it places upon you, your reaction to challenges presented during incidents will also be different. It is a fact that when something worked well for one, it is quite possible that it will not for another. Much of your reaction will be based on your individual perception of a problem. Just as importantly, often situations do not have "correct" or "textbook" responses. Each individual will find a solution that meets his or her individual needs and different methods of applying resolution.

Mistakes or errors happen to all of us. Hopefully, you will not have to make some of the same mistakes and errors experienced during past deployments. There are more than enough new challenges out there to stumble through; you should not plow old ground others have explored. Another purpose of this essay is to demonstrate some of those past experiences and their lasting impacts.

This material is presented only for your consideration when confronted with a new challenge. Some of the items detailed have successfully met the need on past incidents. Some are thoughts about what should have been applied.

None of the material presented is to be construed as policy, procedures or regulations condoned by any agency. These are our thoughts on methods, processes and directions drawn from past experiences of experienced responders that are offered for your consideration. If you happen to develop a few new experiences for yourself along the way, so much the better.

Section 2 - Team Procedures

Some basic procedures are needed to streamline and codify team operations during times of emergency stress. By identifying certain performance standards prior to the time crunch during an actual incident, all members will be able to react with less confusion and in a more professional manner. Some of the areas to consider are:

Written operating procedures

Different Incident Commanders may expect different operations to be performed within a team setting. This is acceptable. However, team members scurrying around trying to figure out what and how to perform operations is not. Each Incident Commander should take time to write out basic operating guidelines, so members understand expectations. (See the Example Standard Operating Guidelines in Appendix F Annex 1.)

How an Incident Commander expects the team to work. This will include meeting schedules and acceptable timeframes (e.g., Planning Meetings lasting no more than 30 minutes requiring everyone to be ready for the meeting). Also included are acceptable get- away times for a dispatch, communication procedures while responding, which team member(s) go to the dispatch center or Emergency Operations Center (EOC)-and retrieve what information, as well as other basic information on what an Incident Commander feels is necessary for the most professional performance by the team. Detailed directions could easily become over-kill. Team specific guidelines should be developed and endorsed by all team members. This buy-in is paramount.

Position specific expectations the Incident Commander has for team members

We all know the duties and responsibilities that position training delineates for each role. Position specific expectations reinforce and place additional specific responsibilities on each position. These types of expectations, when stated, give a person clear direction. These expectations can be as detailed the Incident Commander desires, so that he or she is comfortable that all areas of concern are clearly assigned to specific team personnel. It would be helpful if position expectations also included the Incident Commander's own role so that all personnel understand what that person sees as the primary responsibilities of his or her command position. Position statements should also include direction to those personnel the Incident Commander expects/requires written summaries from for inclusion in the IMT's Narrative Report.

Explanation and examples of Performance Rating that will be used by team members.

It is highly recommended that each Incident Commander mandate a rating process for all team members and other personnel who are assigned to an incident. Specific responsibilities delineated in team guidelines should be individual rating factors for the specific position.

Pre-Incident Communications

Intra-team communications are key to a smooth operating group during an incident. Incident Commanders will find communications during incidents will flow smoother if members have routinely shared information prior to a deployment. An Incident Commander should take the lead in facilitating this flow. This can be as simple as utilizing email and social messaging to send information that could impact team performance during an incident. Developing a team phone list with all member's pertinent contact information (cell, and work numbers and email address) will also assist personnel with communicating. One thrust of these communications is to keep all members apprised of changes and news; another is to develop the group into more than a collection of people. The word "team" comes to mind; the goal is best team interactions possible.

Continuing personnel development

In complex incidents the Incident Commander and the agencies supporting response can't afford placement of personnel onto an IMT that are too inexperienced or unwilling to perform at a high level. The reasons for this should be obvious. Therefore, it is incumbent upon all Incident Commanders to facilitate an environment within their respective teams that provides the best "hands-on" personnel development possible. After all, who is better suited to be the Planning Section Chief in a major incident than personnel who have repeatedly and successfully worked in a Planning Section unit-level position for major incidents? Just being exposed to the dynamics of another position during an actual incident must be some of the best training agencies can provide. This exposure should include development of selected personnel for the Incident Commander's role. Some other personnel development ideas to consider:

- Complete Position Training: ensure that currently assigned personnel have all necessary position training for their position. Require new assignees to meet these standards.
- Encourage/Require Mentoring: functional leaders should "step-back" as incidents allow so that subordinates may perform as a well supervised "lead person" (e.g., the Situation Unit Leader becomes the acting Planning Section Chief during stabilization or mop-up of an incident). Team members must consider "mentoring" as a key important role.
- Enable a "Team Building" atmosphere: Encourage the command and general staff to delegate responsibilities and authorities where appropriate. This will require the Incident Commander to do the same.
- Cross Train: Team members become much more valuable when cross-trained in multiple functions. Knowledge of the other jobs is needed.
- Develop multiple qualifications: e.g., Situation Unit Leader also qualified as a Food Unit Leader or Finance Section Chief as a Safety officer with accident investigation experience.
- Develop Talent: be proactive in recommending advanced position training for those team personnel who successfully perform their positions and demonstrate abilities for future roles.
- Maximize use of Trainees: keep all allocated trainee positions full for each deployment. Each team member should strive to make a trainee assignment as meaningful as possible for participants. Once a trainee has demonstrated knowledge and abilities to perform in a position, that person should become eligible for placement onto an IMT and another person afforded the trainee slot to develop their skills.
- Train Internally: Encourage the qualified team personnel to be involved as instructors for training of others. A person naturally becomes more proficient when giving instructions than receiving them.

- Give Performance Feedback: require performance ratings for all team members during activations. One theory of such ratings is to identify a person's preparedness for advancement as well as identification of areas requiring improvement.

Post-incident critiques

Post-incident critiques for all team members must be performed. This should become a standard team process. Identification of areas that went well and those requiring improvement, what material items are necessary for the next activation and any additional training requirements of members are but a few of the desired outcomes. This will enable the team to build towards an improved response for the next activation.

A component of post-incident critiques is collecting performance information through debriefings. One approach could be a directive announced during Operational Briefings that all persons assigned above a certain position (Division or Group Supervisor, as an example) must report to a designated location upon relief for debriefing. However, if this is announced, someone from the management group must be at the location until all debriefings are received.

Professionalism

One goal all team members should strive to attain is bringing the highest level of professional management possible to an incident. This concept is difficult to define in that there are as many thoughts on what a "professional" management group is as there are people to ask. Clearly, your agency expects and has the right to accept nothing less than a group performing management tasks during an incident in a manner that will bring only the highest respect from all observing persons.

When developing a professional atmosphere take into consideration that team members must know their jobs, roles and required interactions. Obviously, this will entail all members to be position literate and to understand what is needed to communicate and perform well within a team setting. Being literate of other functions will reinforce the timely and essential transfer of proper information. Written team guidelines further describe specific tasks, communications and relationships that are expected of them.

A professional team will ensure that team members are easily identifiable. Any person on or around an incident site should be able to easily identify the incident's management group by name and position. Rapid procurement of standard identification items (e.g., hats, name tags, vests) must be done as new members come onto a team.

Punctuality is a mark of professionalism. All team members should adhere to punctuality in all actions. If a Planning Meeting is set and advertised for a specific place and time, the meeting must begin at that time and place, regardless of who is missing. This will aid in setting the "tone" for all observed actions conducted by a team. It clearly tells all: "this group means to approach the profession of complex incident management in a businesslike

manner." All other actions must also be punctual and purposeful. Routinely, a person will only be late for one such meeting if there is a standard method of recognizing tardiness.

A professional team communicates effectively, providing continuous timely and meaningful interaction with the responsible jurisdiction or agency. When invited, an IMT is a guest expected to perform a mission. By transferring information to the responsible jurisdiction throughout the incident, the IMT reduces the questions that always seem to arise after the fact. Communicate effectively during the incident with those persons that will be left to recover in its aftermath. This need for communication will not be limited to the Incident Commander's position. Team members must consider themselves an "extension" of someone from the responsible jurisdiction; find out who this is and develop a rapport. This is the person(s) you want to be pleased at the end. Another aspect of effective communication is that team members must be approachable and open to input. This sounds simple, but it is not an action always seen. The personnel on an incident have experience – they have "been there." Team members need to listen to what experienced responders have to say. Learn from their experience.

Situational Awareness

It is important to provide information to all participants in the incident response. Ensure that Incident Action Plans (IAPs) are available to all that need them. Is it correct for a management group to decide personnel below a certain level of the organization (Division or Group Supervisor, as an example) do not need access to the IAP? Watch what happens when there is a serious accident and investigators ask surviving responders if they knew the plan of action or communications for the incident. If time or machines don't allow timely reproduction to meet this demand, consider the use of QR codes, digital pictures, or posting copies of the IAP. This will allow any interested responder with the opportunity to review it.

Make sure to use information displays effectively. Visual presentations, (e.g., displays, dashboards, monitors, maps, etc.) are an effective method of communication. Posting the current IAP as well as information on the next operational period (when available), news from the world outside the incident, weather, meeting schedules and required attendees are but a few informational items to consider for displays. How about posting directions to drop points, the Medical Plan, and an updated Safety Message, vehicle parking directions, the menu of the day, etc.? Think of visuals as a tool: a team does not have time to verbally relate everything individually to every responder on an incident. But everyone needs and wants to know incident information. Assume they can read!

Orderly and complete paperwork

Time records, documentation package, fiscal records, and a team's Narrative Report are just a few of the written documents which will be available forever. They should be written to effectively relate the story of the incident – an Incident Management Team came, they conquered, and they left. Make sure you go down in history correctly! Addition of internal audits and/or settlement of a cost apportionment only adds to the possibility your historical

documentation will be received by a vast number of people. Don't let an excellent job performed under adverse conditions be judged poorly later because you provided substandard documentation.

Section 3 - Transitioning

Transition is transferring responsibility for an incident to an IMT. The definition of the transition includes: "a process to familiarize a group of persons to a situation in progress as well as setting strategic priorities for its control." For an IMT, this situation they are responding to is often a major complex emergency incident, and this familiarization is to gain real-time knowledge of the incident along with local operating procedures for the team. Pretty straightforward, right?

Think about the act of transitioning an incident to a team. It hasn't been a good day. All efforts to control the incident are not going well. The incident has exceeded the on-scene capabilities or capacities (or you wouldn't be there). Not only is the incident not going well but, by the time the team arrives, there can be tremendous amounts incident-caused property loss, injuries, or deaths.

Agency Administrator Briefing

You normally will be dealing with an Agency Administrator who may or may not have been part of the decision to activate your team, and you might be strangers to this jurisdiction. The Agency Administrator is trying to deal with an unfathomable number of details and/or possible political pressures. He or she will want one thing from the IMT: MAKE IT BETTER!

What the IMT needs from the Agency Administrator is all necessary pertinent information, official authority to perform their mission and direction to go to work; the faster the better. Obviously, if a transition isn't done efficiently, something important could easily be lost. Missed items at this point will be detrimental to the incident, impacting a team's efforts and recovering them could be difficult. A rapid transition could well be the worst action taken on an incident.

To avoid "dropping the ball," transitions should be approached in a clear and systematic manner that transfers the most information possible. Documentation of this transfer is needed for later reference. These documents will become the cornerstone to an IMT's actions and written history of the incident.

Teams should also view the transitioning process as an opportunity to make that lasting "first impression" upon the responsible agency. Don't miss this opportunity. So, with all the hazards identified, how is a transition done to minimize adverse impacts? Some issues to consider:

The IMT should have a pre-prepared format to utilize for the Agency Administrator Briefing. Use of a standard transition agenda or checklist provides a good method to ensure transfer of key information identified from past deployments. The questions on a checklist ensure

that the Agency Administrator will contemplate and respond to information requirements for the IMT that might otherwise go by the wayside.

A best practice is for the team's Incident Commanders to conduct a yearly review of this checklist to incorporate new information items that have surfaced from recent incidents.

Most agencies have some form or format for the Agency Administrator Briefing to an incoming IMT. States and other departments may have a different version of the form. Some jurisdictions have no form for transition. The Reference Guide includes a sample Agency Administrator/Executive's Briefing Checklist on page 151. When responding to an activation, the Incident Commander may want to call the responsible agency to see if they use a specific transition format. If no transition form is used by the responsible incident jurisdiction the Incident Commander may suggest they consider using one and email a copy, followed with confirmation it arrived. A best practice is for the IMT to maintain their own AA Briefing Checklist in case the Agency Administrator does not have one established. The IMT Incident Commander should conduct a yearly review of this checklist to incorporate new information items that have surfaced from recent incidents.

During deployments, teams should expect the form to be incomplete and lacking a depth of information. It is not unusual for the Incident Commander/team and Agency Administrator to jointly fill out the form. This may require some education (for both parties) and negotiation. There could be instances where the form will not work at all. However, it can serve as a guide to develop some other mechanism of pertinent information transfer and documentation.

Transition using a formal Agency Administrator Briefing takes place at a specified time and location utilizing the completed briefing checklist. Negotiation by an Incident Commander may be necessary on timing of this. A vast majority of team members need to be present for the transition. Travel times for some members could require transition to be delayed beyond a responsible agency's expectations. This will be especially true on incidents where agencies expect a team to assume command upon arrival of the first member. It will be incumbent upon the Incident Commander, with the Agency Administrator's assistance as necessary, to negotiate a realistic timeframe that allows proper personnel to arrive.

The team needs to ensure they are setting a professional tone for the Agency Administrator Briefing by being punctual, identifiable, prepared, and attentive. Prior to the briefing, the Agency Administrator and Incident Commander should have set an actual time for team actions to begin on the incident. This should be a portion of the briefing. If not mentioned, this will be one of the questions to bring out.

All team members should be identifiable using well-marked Personnel Protective Equipment (PPE) or their agency's work uniform with issued team identification clearly displayed. The team members should form a group close to the agency speaker with the command, and general staff in the front. Team members should all have notepaper and a writing instrument, or an electronic device to take briefing notes. Ideally, a copy of the completed

transition checklist will be available. If a completed checklist is not available, a blank checklist can serve as a guide for team members to generate questions pertaining to their specific roles. It is not unusual to have many people other than the IMT and key agency personnel present. Determine who everyone present is and understand their assigned role.

An Agency Administrator briefing should start with introductions of the key agency personnel by name, title, and incident function. Teams should introduce themselves by name and ICS position. Routinely, the Agency Administrator conducts the briefing with an overview of the incident's history, projections, resources status and conditions. However, a team should be prepared to assist this effort.

After the Agency Administrator briefing, the Incident Commander should negotiate a question period for team members to retrieve necessary information that might have not been dispensed. It may be best for the Incident Commander or Planning Section Chief to facilitate this portion, going through team functions (e.g., "Resource Unit Leader, any further questions?"). Team members need to be prepared with questions restricted to the pertinent issues needed for their position and function. Lastly, collect any written materials or displays presented to the team by the Agency Administrator, regardless of whether they initially appear to have value.

Team members should view the Agency Administrator Briefing as the opportunity to make a lasting "first impression" on the requesting agency or jurisdiction. This could quite possibly be the first meeting the Agency Administrator has ever had with any member of the IMT. As an old saying goes, "first impressions are lasting impressions." Take every opportunity to leave the impression that a first-rate professional management group is there to perform a required mission.

Delineation of Roles and Authorities – Administrator's Letter of Instructions

Terminology: The Administrator's Letter of Instructions is commonly referred to as a "Delegation of Authority" but may also be called a "Letter of Intent," "Letter of Expectations" or "Letter of Direction." For the rest of this document, we will refer to it as a "Delegation of Authority" following the language in the Reference Guide (a sample Delegation of Authority is included on page 153).

A signed copy of the Delegation of Authority should be given to the IMT, along with the Agency Administrator Briefing form. These documents clearly set team actions into motion. Roles and authorities become extremely important for team non-agency incidents as well as for non-wildland fire incidents (e.g., mobilization centers). When an IMT is requested, immediate contact should be made by the incoming team's Incident Commander to the Agency Administrator to explain the transitioning process including the Delegation of Authority.

Remember, some jurisdictions don't routinely transition incidents to teams, and this could easily be the first such occurrence. Your expectations may be severely shaken if you assume

that your incoming IMT's routine will be known by the jurisdiction and that the transition will take place smoothly. Special attention should also be taken when a team activation is for an assignment other than assuming command of an incident. When a team deployment is to provide management for only a part of an incident, this should trigger an alert for you to ensure specific roles and authorities are very clearly identified. As an example, during a major multi-county flooding incident, a team is deployed to manage the care and housing of evacuees only and will not take part in the overall management of response to the incident. For an assignment like this, an IMT would need their specific roles defined and a clear understanding of their authorities.

An IMT will routinely find that requesting jurisdictions will not be familiar with the full capabilities of the team that they have requested. However, there is an acceptance by the jurisdiction that a team does know its own capabilities. Based on this assumption of team expertise, the jurisdiction will normally be willing to act on, participate in and provide what the team suggests is needed to manage the incident.

One of the best ways to demonstrate professional leadership during response to other jurisdictions is to "walk" the jurisdiction through the Agency Administrators Briefing and assist with the completion of the Delegation of Authority. Time taken to walk the jurisdiction through these documents at this first meeting will reap benefits throughout the deployment. This is also the time to determine if all the jurisdiction's key personnel are informed of and involved with delegation/direction to a team. Count the noses and determine if all key folks are involved. For example, there is nothing worse than to discover that someone forgot to tell the sheriff that an IMT is being brought in to manage a flood within the county. The sheriff is the highest elected peace officer in the county. He or she might not necessarily subscribe to the notion that help was needed at all. A key elected official that objects to the presence of an IMT can be a significant obstacle. This may be the only opportunity to gather information before the team assumes an incident. Go slow. Be thorough. Try not to let key players get away before you have gotten all your questions answered. Refer to pages 146 and 154 for more information on the AA Briefing and Incident Briefing.

Incident Briefing

It is important that the Initial Response (Initial Attack) Incident Commander who is currently managing the incident also briefs the incoming IMT. The most current incident situation status should be available from this person and his or her staff. Many times, this briefing is conducted concurrently with the Agency Administrator briefing. This has pluses and minuses but is normally something a team cannot control. Some expectations will be that the team will need the best incident information available, e.g., what has happened, what has been tried, and any projections of incident size, resource status, locations, and serviceability. Situation maps, weather forecasts, traffic maps, and ICS Form 201, *Incident Briefing* (refer to page 241) if available, should be obtained. The team will need direction on future involvement of agency personnel currently on the incident. Do they stay to be incorporated

into the incident's structure or are they to be released and when? This is decided between the Agency Administrator and the initial Incident Commander.

Teams can leave a lasting positive impression if a request is made to have a "local" person assigned to them for the purpose of local knowledge availability. Routinely, they will want the initial Incident Commander to stay assigned and available to the team. This person had the agency's trust to manage the incident up to this point; an assumption must be made that he or she is the most qualified person the jurisdiction had available.

A word of caution: information from the initial Incident Commander may not be complete. Some become overwhelmed and fatigued because the incident escalated to the point of having to bring in a team. A lot of negativity can be present that could distort a team's perception of the incident before they see the situation for themselves.

Initial Strategy Meeting/Command and General Staff (C&GS) Meeting

Upon completion of the Agency Administrator Briefing and an Incident Briefing, team members must assemble as a unit for the purpose of confirming the information received and conducting an Initial Strategy/Command and General Staff (C&GS) meeting. See the *Example Initial Strategy/Command and General Staff (C&GS) Agenda* at the end of this section. Refer to pages 124 and 170 for more information.

As noted in the Reference Guide, the All-Hazards community places this meeting in the stem of the Planning P (Initial Response) to highlight that there are actions specific to the initial Strategy Meeting that generally do not occur in later Strategy Meetings.

In this meeting confirmation of received information and materials should be done so that all team members start on the same footing. Just as everyone seems to hear an item differently, group knowledge could be disjointed. Do we all have the same information and, if not, how do we get differences ironed out? Take some time to confirm that the information you have is the same information everyone else on the team has.

To facilitate team actions, a general strategy for the team must be established based on the most current incident status (refer to ICS Form 230 on page 250). This could be as simple as all functions checking on actions to this point that will affect their roles, or it could be setting a time for the first Planning Meeting should the team be assuming immediate command.

The Initial Strategy Meeting develops the realistic and verified Common Operating Picture that incoming IMTs must gain during the transition/transfer-of-command process. This requires distinct efforts. "Ground Truthing" is comparing what they were told during the Agency Administrator's Briefing and Initial Incident Commander's Briefing with what the team members were able to see. This and sharing the Essential Elements of Information (EEIs) that each member has collected in the initial phases of the transition/transfer-of-command process are critical to a team's success.

The Initial Strategy Meeting can also be used as an information sharing meeting.

This meeting should clarify and help to ensure understanding among the core IMT members of the decisions, objectives, priorities, procedures, and functional assignments (tasks) that the Incident Commander/Unified Command (IC/UC) has discussed and agreed upon.

Examples of critical information that is shared in the Initial Strategy Meeting:

- Organizations that need to be represented in the Unified Command (if established)
- Leader(s) Intent
- Limitations and Constraints
- Name the incident
- Objectives
- Setting the Operational Periods/Duration
- Meeting and Briefing Schedules
- Identification of external influences – Social, economic, political, cultural
- Defined IMT Operating Procedures. In the initial response the IC/UC must establish guidance for the conduct of operations in the incident. These should include:
    - Assisting and coordinating organizations that are needed to carry out the IC/UC objectives
    - Integrating Assisting and Cooperating Agencies
    - Identifying support facilities and locations (Incident Command Post (ICP), Base, JIC etc.)
    - Sharing the details of the delegation of authority with team
    - Providing direction for information flow and release
    - Providing directions for sensitive and classified information
    - Providing directions for resource requesting/ordering process
    - Providing directions for cost sharing, and cost accounting
    - Providing guidance on managing operational security issues
    - Determining Command and General Staff composition, including deputies (especially OSC and PSC)
    - Providing IMT functional assignments
    - Determining UC functionality and spokesperson
    - Defining Incident within an Incident procedures
    - Identifying Critical Information Requirements (CIR) reporting requirements

Example Agenda for the Initial Strategy Meeting/Command and General Staff (C&GS) Meeting

1. PSC brings meeting to order, conducts roll call, covers ground rules, and reviews agenda

2. SITL conducts situation status briefing

3. SOFR provides safety status briefing highlighting any near misses or injuries requiring medical attention beyond first aid and ICP/Base/Camp safety issues

4. IC/UC:

   a. Provide comments

   b. Review priorities, limitations, and constraints (if new or changed). Reviews key decisions and IMT Operating procedures (if new or changed)

   c. Discusses incident objectives

   d. Reviews Critical Information Requirements (CIRs) and their time criticality

   e. Presents or reviews functional work assignments (tasks) to the Command and General Staff recording on the Incident Open Action Tracking Form (ICS 233-CG)

5. PSC facilitates open discussion to clarify priorities, objectives, assignments, issues, concerns, and open actions/tasks

   a. OSC provides update on current operations.

   b. LSC provides update on logistics major issues, such as facilities, communications, medical, food, and ground support, and supply.

   c. FSC provide update on impacting finance issues

   d. PIO provide update on media issues

   e. LOFR provide update on assisting and cooperating agencies

   f. SOFR provide risks and mitigation issues

6. PSC Reviews status of open actions and work assignments (tasks) from previous meetings. (ICS Form-233 CG *Incident Open Action Tracker*)

7. IC/UC provides closing comments

8. PSC covers next meeting and planning process assignments

NOTE: DOCL documents meeting and distributes meeting materials

Subsequent Strategy/Command and General Staff Meetings

Depending on the organization that you are in, later meetings may be called Strategy Meeting, C&GS Meeting, or an information sharing meeting. These can be held as needed and are used to decide how best to meet the incident objectives. These meetings may cover

any changes in command direction, review open actions and status of assigned tasks using the Incident Open Action Tracking Form (ICS Form 233 CG on page 250), and revise operating procedures. Examples are changes from the Agency Administrator, critical resources issue, major change in strategy, Incident within an Incident ramifications.

The Strategy/C&GS Meeting occurs prior to Tactics Meeting. The meeting is facilitated by the Planning Section Chief. Attendees include IC/UC members, Command and General Staff, Situation Unit Leader (SITL), DOCL, Communications Unit Leader (COML) (if required), Finance/Administration Section Chief (FSC), and the Logistics Section Chief (LSC) (as needed).

Section 4 - That First Operational Period

That first operational period (refer to page 165) faced by an IMT is a kaleidoscope of efforts. Each team function is furiously gathering, exchanging, and disseminating information, formulating plans, and structuring their specific jobs with needed staffing. Initial response personnel need relief and retrofitting, new responders need to go out under direction, incident facilities need development, long-range planning begins and an in-depth review of all safety aspects of the incident is needed. These and many other tasks must be undertaken beneath the pressures of interagency coordination and the ever-watchful eye of the media. Not much happening, right?

The state of the IMT is also a composite of effects. Personnel are routinely working extended hours. They have hopefully gotten their direction and written authority after participating in a Transition Briefing. The incident's setting could be unfamiliar to them. Personnel currently working on the incident may have limited information. Resources and materials of all types are invariably still "en route." Mentally, the team knows what to do and desires to do it. Physically, frustration will set in when incident demands outdistance available resources.

Initial response is often chaotic, and you likely won't have everything you need immediately to bring order to this chaos. Experience will assist in limiting this frustration. Once you've lived through your first - first operational period, the next initial operational period on the next incident is easier to take in stride. Some details initially felt to be critical have proven to be less so. You see that some shortages have been compensated for. Information gaps become expected.

It is not acceptable for a team to just throw their hands up in disgust at the chaos they are facing. The likelihood that an initial start-up of team operations can be a little rough should be understood and accepted. One of the strongest points of an experienced IMT is ability to recognize and adapt to situations thrown at them. Professionally bringing control to chaos during a start-up is one of the brightest attributes and lasting impressions a team can impose on an incident.

Managing Chaos

There are many items to consider for coping with this "first operational period." In the areas of resources and information you should recognize and expect shortages. Resources and information of all types will be in short supply. ETAs of ordered resources/supplies can be protracted. Situation reports or maps may contain little useful information. You may receive unanticipated announcements of important person (VIP) visits. Accurate reports of resources currently assigned may not be available. Timely reports of past injuries, losses or costs will likely all be missing. EXPECT THEM! Anticipate shortages and adapt to work around them.

Remember that obtaining the best available information PRIOR to arriving can attempt to shortstop the "it's lost in the system" syndrome.

Making sure there are well established team guidelines and defined operating procedures can lessen chaos. Directing specific functional roles on the IMT to gather information. Some examples of how to do this could include the following:

Operations: Assign a team Operations person to personally recon the current situation. This may be done rather than attending the Transition Briefing if another Operations representative is present for the briefing. Hands-on review of current strategies, resources and projections will greatly enhance a team's ability to produce a useful IAP when called upon to do so. If a resource such as suppression resources is limited, continue to focus its work on the part of the incident where they will do the best.

Planning: Provide multiple briefings for "late" resources. Direct a team Planning person to the responsible agency dispatch center. Their mission would be to:

- Retrieve copies/digital source of any agency incident situation and resource status documentation developed from the start of the incident.
- Obtain copies/digital source of any news releases, incident cost calculations and weather forecasts/projections.
- Get any information available concerning past incidents within the general area of the current one.
- Determine exact procedures for situation updates and other dispatch contacts desired with contact person(s), methods and numbers.

Logistics: Direct a team Logistics person to routinely go to the responsible EOC. Their goal is to get copies/digital information of all agency documents utilized while gathering resources and supplies and to ascertain exact procedures and identification of contact person(s) for the continuation of ordering/confirmation with pertinent contact methods and numbers.

Burn Out:

A pitfall all team members need to recognize is the potential to work themselves beyond usefulness during the first operational period. Commonly members have been working at

regular assignments when activated for a team response. Travel is conducted to the incident, a transition takes place, and the team goes to work. A team routinely assumes an incident in time to brief and get the second day's operational period to the line. Work continues through day two to prepare facilities, accomplish planning and generally organize a large incident. Even if the incident does not enlarge significantly during day two, team members work all that day to get their functions staffed and performing well.

Studies show that "burn out" occurs at about hour 11 when under stress. In burn-out, efficiency and production decline significantly, thinking and problem solving are degraded, and safety becomes a real concern. Team functions require a mental state capable of simultaneously performing multiple tasks. Everyone has a point of diminishing return regarding the ability to cope with demands placed upon them. Forgotten items become lost, personnel can be left in unsafe situations and needs go unmet. Team members can become exhausted without getting dirty. All members must recognize and be proactive to prevent this.

Some practices to consider for safeguarding against over-extension or burn out of team personnel:

- Divide positions. Team positions having a second person assigned will require a conscious division of workload. Team Incident Commanders may have to monitor this Division to ensure it is working. The person not "on" must try to get some rest to relieve his or her partner at the proper time.
- Adjust the Length of the Operational Period. A compressed operational period can create increased time pressure. Use of twenty-four-hour operational periods has proven to ease compression of time for some functions (e.g., Logistics, Planning, and Operations). Not that the workload goes away, only more time is available in an operational period to accomplish it.
- Utilize Deputies. Team guidelines can require certain sections to have deputy positions filled whenever the crunch of an incident is expected to exceed a certain operational period (beyond the team's second).

Overestimation

Experience teaches us to expect the unexpected. Ordering more assistance is not always an answer either. Being dependent on others opens the possibility of letdown. Availability, travel times or other incidents can severely impact accumulation of more staff. It is a best practice to have an alternative plan available in case the chips don't all fall into place.

A common practice during the infamous "first operational period" is a tendency to overestimate production. While this happens less in the Operations Section, all sections can fall prey. For example, the kitchen's ETA is 1100 hours, and an unknown breakdown delays it until 1600 which impacts feeding of personnel going out. Overestimation can hamper you in your quest to accomplish your function.

Teams should consider the possibility of overestimating their own staff production capacity, especially during that first operational period. Is it possible to draw together a current IAP, be working on the next and correctly look at contingency planning? Can necessary facilities be developed; communications organized and drop points marked with available staff? Can each member realistically accomplish all required actions within that "first operational period"?

Some items to consider in order to avoid overestimation:

- While developing the ICS Form 202 *Incident Objectives* (refer to page 241) for that first operational period, an Incident Commander could list specific objectives and goals for non-Operations functions (e.g., Logistics develops a 2,000-person camp; Finance/Administration ensures all contracted equipment time is started). This prioritizes actions and accomplishments. It also implies recognition of limited resources. A visual display of the objectives and products should be posted.
- Individual section chiefs must prioritize specific work to be accomplished on ICS Form 233 CG. Staffing is routinely still short and only so many "things" can be accomplished; what is most "important"? List them and get them done in that order. Should an individual's priorities impact other team functions (and THEY ALL WILL!) this must be shared with the other team members. A full team meeting four to five hours into that first operational period works excellent for this intra- team sharing of information about projected shortfalls and accomplishments.
- Recognize when the "impossible" is not, it just takes a little longer to accomplish. Most challenges faced by a team when organizing an incident can be successfully met in many ways. Be adaptive and creative while guarding against expending precious time on a scheme with marginal chances of success. A standard "book" answer is not always needed.
- Rely on past experiences (mental recollections) to meet significant challenges. There is a depth of collective knowledge when an IMT is assembled. That first operational period team meeting could produce problem-solving suggestions from a most unlikely source if members are made aware of a difficulty and they feel free to help. Use someone else's experiences when necessary.

Learn to recognize the abilities of other team members. You could and should have cross-trained folks at your disposal. That information officer might also be an outstanding Logistics Section Chief. The strongest attribute of good management teams is an openness to share ideas and work. Too many times a person's focus becomes so narrow chasing their individual challenging demons that they forget that there are a lot of folks on a team, all with the common goal of making the entire production work. Share your needs and ideas. Each incident will impact each team member differently. That information officer might not have a lot to do on this incident due to its extremely remote location and, therefore, could be of assistance to Logistics. At meetings have team members brainstorm and prioritize what needs to be done. Encourage team members to help where help is in short supply.

Section 5 - Communicating

During an IMT deployment, proficient communication becomes extremely important. This includes not only internal incident communications that utilize radios, phones, digital messaging, and face-to-face to transmit information used towards control of an incident, but intra-team communications as well as off-incident transfer of information. Effective communications will directly impact a team's success and the impression they leave behind. Basically, communications can be broken down into three major categories:

- Intra-team (within the IMT)
- Intra-incident (within the incident management including the EOC and the MAC Group)
- External (the public, media, and social media)

Unsuccessful accomplishment of any category will impact a team and incident adversely.

Intra-team Communications

A variety of methods exist to avoid this. Intra-team communicating is the essence of team interaction and requires a conscious effort by all members. It is not that people are excessively introverted but, some do find it extremely difficult to share thoughts and ideas before a group. Some avenues to consider:

- Be Open: sincerely welcome new members to the team.
- Develop a Culture of Communication: efforts must be spent to keep an intra-team atmosphere that advocates smooth and healthy communications. This is easier said than done. Many obstacles can lead a member to be reluctant to participate.
- Solicit Input: Agency affiliation can be a communication barrier. Some team members may be hesitant to actively participate in open team communications until it becomes obvious their input is welcome and, yes, needed. Personal discussions with the Incident Commander or other team members could help; it may take repeated team interfacing for a person to loosen up enough to participate. All team members need to be aware of this situation and ready to rectify it.
- Emphasize Position over Rank: Unfortunately, some folks will hesitate to take part because they are outranked. An Incident Commander should make it crystal clear that, in a team setting, all collar brass was checked at the door; every member is just that a member! Your only "rank" is that afforded to your team position. Again, this may take repeated demonstration by all team members to loosen up the rank consciousness.
- Create a Learning Environment: A person might be self-conscious of what they perceive as a lack of experience or knowledge compared to other team members, subscribing to the theory of not demonstrating this lack by opening their mouths. Again, the team atmosphere will need to recognize that there are as many different

levels of experience as there are members and that's OK. Besides, those with loads of experience had to start somewhere too.

Team guidelines can describe and structure team operations in a manner that clearly requires and promotes the importance of communication in intra-team actions. Teams should develop a standard procedure for documenting all meetings (refer to page 119). Too many key decisions and directions develop during meetings seem to require later review. Bring in a scribe or delegate this task via team guidelines.

Team structure requires numerous meetings:

- Transition Briefing (Agency Administrator and Incident Briefings)
- Strategy Meeting
- Planning Meeting(s)
- Operational Briefing(s)
- Daily Team Meeting(s)
- Section/Functional Meeting (share and post information)
- Demobilization Planning Meeting
- Closeout Meeting (refer to page 213)
- Team Meeting (critique)

It is advantageous to discuss meeting processes in team guidelines. Expectations on length, contents, participants, and needed interactions as well as need for documentation should be explained. Continually drive home the idea that gathering, exchanging, and disseminating information is a shared responsibility of all team members. Ensure a clear process to do this is understood and expected by all. Meetings by team members coordinate a vast majority of team management efforts. They are needed BUT, the number of them can become overwhelming for personnel trying to accomplish something (such as managing an emergency). A watchful eye should track all meetings to eliminate unproductive or counterproductive time.

Position specific expectations within team guidelines can list those types of information required by team members. This alerts members to the nature and detail each other member expects from them. Incident Commanders and Section Chiefs should watch conduct of meetings and member's participation to ensure an open working atmosphere is cultivated and supported.

Having a clear posted agenda with outcome expectation, along with members' knowledge of the expectation of their punctuality and preparedness, should maintain the businesslike team attitude.

A team member assigned as the team's meeting facilitator (team guidelines), could also help. Leave the rabbits for after the incident. Every team meeting should start with, "the purpose of this meeting is _____." The following people must be present _____, _____, _____, _____.

Intra-Incident Communications

Intra-incident communications are those made from the incident to others, off-incident, that are involved in support of the incident. This will include, but not be limited to, briefing the Agency Administrator, working with the EOC and dispatch center, tracking down vendors for specialized items, or transmitting cost information to a suitable source. These and many other communications will say volumes to everybody about the team and its personnel. Therefore, team members need to be aware of the expectation that all communicating will be of the highest professional level. The most off-incident reviewed and discussed document a team will produce during a deployment is the ICS Form 209 *Incident Status Summary* on page 243. Accept this fact. Completeness, accuracy, and timeliness are paramount. There are deadlines for the ICS Form 209 that must be met as this document is used to give resources to your incident. It must be on time.

There are many documents required to be transmitted off an incident. These include ICS Form 209s and cost estimates. Ensure you know them all. Reconfirm a timetable and method to be used with the receiver early during the incident for each document. Significant time can be wasted by too many people tracking down late or incomplete documents. Awareness of the importance of providing off-incident communication by all team members will go a long way to having the team perceived as a structured and accomplished group who can meet deadlines in a professional manner while facing many difficult tasks.

Intra-Incident communications are obviously key to transferring information for the purpose of control. However, even as much as this type of communicating is performed by our personnel day-to-day, there are areas for improvement during major incidents. Keep the incident's personnel or responders informed. We have all been on incidents where no one outside of the incident management's upper echelon had any idea what was going on or projected. Really makes you feel that there was a rudder on those ships, huh? Routinely updated bulletin boards and single page briefings posted where response personnel can easily access them (such as the incident base) are but two of the ways to accomplish the task of informing the personnel. Decide early how and by whom this will be done, then make it happen. Utilize visual displays within the ICP as much as possible. If someone can find their needed information without asking, a manager's time is not spent answering questions. Each team should have some pre-developed "standard" documents available in electronic formats that can be used as needed. Motel policies, personnel standards of conduct, and release priorities are but a few of the documents consistently used incident-to-incident. Teams will develop more upon each activation. Availability will ensure use.

As a communications plan develops, ensure all pertinent information is on each ICS Form 204 *Assignment List* on page 242 as well as the ICS Form 205 *Communication Plan* on page 242. Complex incidents require complex communication plans. The ICS Form 204 reflects the Communications Plan specific only to the assignment of resources to that Division or Group. However, reassignment of personnel about the incident during an operational period affords everyone information needed to properly communicate.

Additionally, ICS-215A (*IAP Safety Analysis* on page 247) information developed should also be on each specific ICS Form 204 Assignment List for the same reasons. Build in flexibility while keeping personnel informed.

Each IAP should include a listing of staff contact numbers. Begin building a cell phone/pager directory early and update it with every new IAP (yes, over 2 million pagers are still in use). Teams should have one started in their laptop computer prior to an activation. In areas with adequate cell phone coverage or made to have adequate coverage when you brought in that portable cell on wheels (COW), radio traffic will be freed up for important operations-based communication. In areas of highly concentrated cellular telephone coverage (heavily populated or with major transportation routes) cellular companies have portable cells as well as large numbers of portable phones available. FCC licensing for these high use areas normally requires companies to provide this service to responders without cost (including the cost of the calls made) during times of disasters. Check with your Logistics folks to ensure they know how to access this service when needed. Some internet providers will provide access free of charge during an incident. Check on it if this could be of value.

An IAP that cannot be read is less than worthless. Its construction wasted a lot of valuable time, and it isn't worth carrying. Recognize that IAPs must be reproduced; reproduction requires a clean original. At present, the cleanest way to develop an IAP worthy of reproducing is to employ computer software systems (e.g., eI-Suites, NIMS IAP, cloud-based networks) Get one and use it! To meet the need prior to the system's arrival, copies of this program are available for personal computers (laptops) which should be in every Planning Section Chief's possession. If an IAP must be handwritten, find someone who can write legibly and produce the best IAP possible. IAP maps are also a problem to reproduce; the GIS mapping system cranks out great maps in 8-1/2 x 11-inch format that can be reproduced with outstanding results. Use it!

Use of the radio for Operations messages enable others to eavesdrop. Operations Leaders (Chiefs, Directors, Supervisors, and Leaders) must be aware that certain communications should NOT be conducted via cell phone. It is entirely possible to isolate a large segment of an incident's organization by not using common communications methods for information needed by many. For instance, if one Division had a serious escalation in conditions and reported this via phone only, would adjacent Divisions (or anyone else on the incident) have all information necessary to them? Certain items need to be heard via common communication methods. Operations Leaders and incident dispatchers need to maintain radio discipline on the incident. Not only will this eliminate untimely use of congested airwaves, but it should also maintain a professional sounding incident for all those listening (like an Agency Administrator or the media). Refer to page 243 for ICS Form 209 Incident Status Summary.

Section 6 - So, You're in Unified Command. Now What?

It is common for significant incidents to involve more than a single jurisdiction. This is an accepted fact and management of these types of incidents has been addressed under the Incident Command System's provision of Unified Command (refer to page 22 on Unified Command and page 157 for Unified Command Meeting). What impacts can an IMT expect under Unified Command? What are some of the pitfalls and what are some "tricks" to making it work?

When transitioning into an incident which is being managed under Unified Command, some alert bells should loudly sound.

- Is this legitimately a Unified Command Incident? Unified Command was designed to "allow all agencies with responsibility for the incident, either geographical or functional, to manage an incident." Do you have such an incident? If not clearly understood, ask your Agency Administrator for clarification. You need to know when an agency is including (or pacifying) a cooperator in Unified Command when the cooperator has no jurisdiction or functional responsibility for the incident.
- Has a single ordering point been set up? The quickest and longest lasting way to adversely impact a Unified Command incident is to have involved agencies continue processing orders for additional resources/supplies through their normal channels. Incident personnel delegated as having overall incident responsibility for their agency (members of the Unified Command) must immediately agree what method (single point) will be used for such ordering, advise their respective agency, and ensure all incident personnel from their agency know of and abide by this decision.
- Is this a cost apportionment incident? This will be a tough topic to broach. However, it is one that needs an immediate answer. Some agencies do cost sharing as a matter of policy; others will not have a clue what this is about. With "…responsibility for the incident…" should come some expectation of financial support for that responsibility. Impasse on this subject must be referred to your Agency Administrator at once. If there is to be a cost share of the incident, some tools are necessary:
- Have Finance Section Personnel been ordered? Very seldom will personnel from the team's Finance/Administration Section have time or expertise required to produce an agreement necessary for cost sharing. Get the help you need. Each agency should be represented.
- Do you have on-hand necessary maps accurately delineating each agency's area of responsibility? If not, get them. If you are not intimately familiar with the areas, have your Agency Administrator or a designee verify the map's accuracy. This is important!

Okay, so all the immediate bells went off and you got satisfactory answers to the first issues. Now what? To proceed smoothly, some preliminary actions, which are different from a single agency incident, are necessary.

Objectives

You will need to establish Unified Command's objectives for the incident that meet all involved agencies' needs. This could be understood as necessary by your counterparts, or it could be an entirely new concept. Availability of a blank ICS Form 202 on page 241 could aid in this effort. Keep the development clearly as objectives, not tactical actions.

Organizational Structure

Once you have established clear objectives you will need to establish the management staff who will fill the Lead Section Chief and Officer roles. An IMT Incident Commander can be intimidating here as he or she just showed up with a whole fleet of highly regarded personnel who normally operate as a high-performance team. Should all agencies choose to use the IMT intact, this job is done. However, should another agency feel it is necessary to insert staff from their agency into the management structure, things can become a little more complicated.

Some avenues to consider while staffing the management structure are to keep the bulk of the IMT intact as "lead" person in each function while negotiating for a limited number of deputy roles for other participating agencies or organizations. Normally emphasis will be for another agency's person in the Operations Section Chief role. Can your team function correctly if the team Operations Section Chief becomes a Deputy? This will be a question each team Incident Commander will have to answer for themselves and their team.

Make sure your Agency Administrator reviews any negotiated staffing settlement. Should qualified personnel from another agency be available to fill all "lead" roles, your entire IMT could become deputies. This will need to be immediately reviewed with your Agency Administrator; he or she might not have brought you in with this in mind. The issue is thrown back to the administrators from all involved agencies for settlement. It's not the best avenue for a team, but it could be the only way to settle it.

Information Management and Incident Facilities

Once the Unified Command staffing is resolved, there are other issues. All the involved agencies personnel will need to establish information release procedures for the incident. All agencies on the incident will need to agree to a single source for development of information released. The Public Information Officer may well have personnel from all involved agencies but released stories must all be the same. This can become the second leading source of problems within a Unified Command setting if left to chance. There will also need to be mutual agreement on incident facilities, location, purpose, and size.

Team Integration

Once the members of the Unified Command come out of their meeting and announce the outcome of their agreements. Now what? If the IMT is to be the "lead" group or if the team is the only command structure present except the other agency(s) members of the Unified

Command; team attitude will set an everlasting tone for the incident. There is a new player in the position of Leader; could there be several?

Team intra-actions must continue as normal. React equally to all members of the Unified Command. This is easier said than done with some. There will be some agency specific needs which might have to be met by staff, and at a time when just what they need is more to do. These are examples of the "little" things which could, with the best intentions, derail a Unified Command.

Any questions concerning conflicts of direction should be immediately referred to the IMT Incident Commander for resolution. All team members must want the other members of the Unified Command to say after the incident that "the team took me in and accepted me as a full member." Remember to be open and honest with your counterparts. Whatever command structure agreed to will have to work and work well. The attitude and cooperation by the IMT cannot become a basis for problems.

Realize that you may be training your counterpart in his or her functional role. IMTs have qualified, and experienced personnel assigned; other agencies may find it hard to match up person-for-person. All team members should expect being relied on to pass along some of this hard-earned experience. It can become a full-time task. Remember, you may well be developing a future member of your team. Remain approachable and open to input. For many of the same reasons as providing on-scene training to counterparts, team members must demonstrate untiring desire for input and interaction. By setting an example of cooperation, a team will stimulate and maintain a desire in all to work together in a common cause. With minor exceptions, all management functions must be collocated. This includes the ICP. We have all been on incidents that clearly had multiple ICPs yet were called "Unified Command."

Finance/Administration is often a challenge for team integration. Here are a few hard-earned thoughts that could make future Unified Command incidents easier for a team when establishing agency specific Finance/Administration personnel within this section. Successful integration may only require an agency Deputy to the Finance/Administration Section Chief to ensure proper procedures and documentation are followed for each agency. You can also establish agency specific time recorders within the incident's Finance/Administration Section. These people work and report to the Finance/Administration Section Chief. However, specific time recording requirements of each agency can be met. You can also establish agency specific Compensation/Claims personnel within the Finance/Administration Section. Depending on which agency's jurisdiction a claim might originate from, the process for submitting claims could be different. By having a person from that agency handle the claim from the start, settlement delays will be avoided. Again, these people would work for and report to the Finance/Administration Section Chief.

An additional challenge is in the area of cost apportionment. Within a Unified Command you might be involved in a cost apportionment agreement. This defines how costs of the incident will be apportioned (shared) between participating jurisdictions, agencies, and organizations. This assigning of percentages is done by the members of the Unified Command. Whenever the members of the Unified Command do this, it should be done in private with the cost share technicians, only. Too much pressure is imposed on an Incident Commander if someone from his or her agency is present/observing; especially if this is their supervisor. Operations Section Chiefs have an important and pivotal role in cost share agreements. They will have to verify, at the end of each operational period, where each resource was used during that operational period. This should be made known early so they may employ whatever means necessary to track resource use. If you are involved in a cost apportionment agreement keep in mind that a Division-by-Division percentage split is needed for each operational period of the incident. Should there be air resources involved, air operation branch directors will have to do the same.

Section 7 - Some Other Things to Consider

Some issues have arisen over the course of past IMT deployments that could surface again; these warrant consideration as you seek to gain experience.

Resources

When there are multiple incidents with competing resource demands, the priority of giving you a scarce resource could be very low. Resources (especially limited resources) are going to be very few and far between. Expect over-using the resources you do have and long delays on resource orders. Even items like the Incident Base will be limited at times. Plan accordingly. Your creativeness and flexibility will be tested. DO NOT resort to hedging reports (e.g., ICS Form 209) of your situation in an attempt to change your priority. These embellishments seldom work as you hope. Accept that some incident must be on the bottom of the list; it's just your turn. Live through it and see how the team's collective imagination produces results despite resource shortages.

Media

What if you have a significant incident near a major media center which attracts a lot of attention. The team's Public Information Officer is doing a good job; however, you can expect repeated requests to interview the Incident Commander. In today's world, the media eventually want and need to hear from "the person in-charge." Consider an organized news conference to fulfill this demand. Advertise a conference time which will meet most deadlines of the media present, find an area of adequate size, get good visual aids, and brief the presenter(s) on the latest status and other areas of public interest. The team's Public Information Officer should facilitate the conference by opening with an explanation that there will be a situation overview and a question-and-answer period; all to be done within a set timeframe. Reporters from most major media sources will understand this

format and process. However, the Public Information Officer should be ready to "rescue" the Incident Commander(s), if necessary.

Below is media guidance written to for a wildland incident. The same principles and concepts can be changed to almost any incident.

Situation: You have an incident with a significant number of structures destroyed. Lucky you. While firefighters did their best, the incident "took" xxx number of structures. Now what? Give specific instructions to all Public Information Officers: their theme is "firemen SAVED xxx (number) of structures, unfortunately, the fire DESTROYED xxx (number)." Note for PIO on language Firemen DO NOT lose structures; we save them! Also, you will need to organize a triage group to rapidly count foundations. Media want a number and will harass the Public Information Officer until given one or will develop their own from any talking source around the incident.

Evacuations

You have to recommend evacuation of citizens from the incident. Alert bells should be loudly sounding now.

The decision to order evacuation is made following state and local statute by elected and appointed officials. Typically, this is a law enforcement responsibility to enact and enforce. However, they don't have knowledge of incident spread that you do and will be relying on you to trigger the need. Get the highest-ranking responsible law enforcement Agency Administrator you can. Figure out where this person fits into the ICS organization. This may include a position within Unified Command or a management position within Operations Section. Responsibilities are evacuation, traffic control and security as well as their routine duties. Make this person feel a part of the incident's organization by involvement throughout your planning process and IAP implementation. Make sure this person understands you consider him or her as the law enforcement head for the incident that is working within your structure. You will want to bring in the local emergency management coordinator (or someone with these responsibilities; different titles exist). This person has (or should have) pre-planned evacuation centers located, contacts with appropriate social response organizations (e.g., Red Cross) and mass transportation contacts. Develop an appropriate level within your organization for this person and delegate necessary responsibilities. This will be easy in those locations with an active disaster planning effort. It is likely an EOC will be established.

If evacuees are placed into incident generated shelters, have your Public Information Officer place a team information officer into each shelter. Evacuees will need periodical updates of the current and projected situation. A uniformed person from your staff is best. Negotiate early with the law enforcement representative procedures (re-entry plan) to be followed once your situation allows reoccupation of the area. Make sure all staff know how this will be announced and what preparatory steps are needed. Law enforcement makes the actual evacuation; they should announce and coordinate reentry. There can be pressure (even

unvoiced pressure developed within the team) to get people back into their residences as soon as possible. Guard against inhibiting operation's efforts and/or possibly needing to evacuate again (very bad)! Human nature will want to get folks back in quickly; just don't make it too fast. By the same token don't delay unnecessarily. The occupant can help the operation by being present.

Re-Entry

Determine as soon as practical the identification of those structures destroyed. Addresses, assessors plot maps or anything else, which will positively locate the structures, will aid in this. Assuming the area has been evacuated and residents have not been allowed back due to on-going control activities, you can set in place some processes to ease this situation for the citizens involved. As soon as Operations can work around limited traffic, announce availability for firefighter-escorted trips during specified times for owners of known destroyed structures. Proof of residency should be required. Have agency vans or other suitably marked agency transportation available. Assign compassionate agency fire personnel in uniform with PPE to function as escorts. Outfit the affected citizens in well-marked PPE. Take them to their structure. Reason: too many experiences with this situation have shown that people, even though it is confirmed for them that their structure is destroyed, HAVE to visit the site for personal closure. When performed correctly, this service will generate rave reviews and leave a lasting impression.

To assist in making re-entry a smooth process for everyone involved you should discuss this sort of action with a local mental health department or other appropriate agency prior to implementation. They routinely have excellent suggestions and counselors available for this type of traumatic undertaking. Also, consider having Advanced Life Support available during such an operation. This has proven worth the effort as reaction to individual trauma can be overwhelming for some; plan for it. The media will want to record these returns for human interest. You cannot stop them unless they are considered a hazard to on-going operations (difficult to do if you are taking citizens in). The Public Information Officer could have them elect a representative to travel with the escorts/victims in your vans to get a story that they will share. Or selected victims amenable to media attention could provide this coverage. Check on it. Also, check those that aren't and protect them.

You'll have the need for a damage assessment for structures destroyed. Place an order for this specialized resource when you have some idea of numbers. It could take a while to assemble the necessary staff to do the job correctly. Consider tapping the county assessor and/or building departments for resources necessary to perform assessments; they have methods we don't, familiarity with what is an inhabitable structure, and resources (e.g., plot maps) which could speed the process. Know what you want from damage assessment, count, photos, prevention information, etc.

Community Relations

Community relations is a broad term for efforts to meet the need of local citizens and elected officials to be informed/involved with your emergency mitigation job. This is an unexplained, but inherent mission each management group has. Your incident is seriously threatening the community. Citizens have a right and expectation to be informed by their emergency responders what is happening and being done versus getting this information from the media or word of mouth. One avenue is to organize public briefings within the affected community. You should coordinate any of these efforts with local elected official (city council person or board of supervisors for the affected area). They need to be afforded the opportunity to be present and/or take part in these briefings.

Depending on the incident's size or "feel" for community concern, the first such briefing within specific areas might need to be done by the Incident Commander(s) with help from your Public Information Officer. Repeat briefings at a location can be delegated to the Public Information Officer. You should make available daily updated single page informational handouts developed by Information and dispersed from places of community gathering and with IAPs are generally well received. Announce in the last one to be published those future issues will not be done.

Elected Officials

Long-term or damaging incidents will generate a lot of interest by elected officials. You have a responsibility to brief them also. When briefing elected officials, you will want to make sure responders themselves know the big picture and have guidance on what talking points they can say if contacted by the public, the media, and officials. Check with a suitable source to decide if the entire group of community elected officials (city council/board of supervisors) would entertain a briefing during a public comment section of their organized agenda. This assumes their regular meeting day would be of benefit (incident is still active). Recommend the Incident Commander(s) make these presentations to community elected officials.

Some items and techniques that will benefit the Incident Commander when giving these presentations are:

- Visual displays will greatly assist in such presentations.
- Don't get too technical. These are laypersons, not responders. They will be most interested in damages done, projections for control and problems encountered.
- If you are unfortunate enough to have an incident that remains active through another scheduled meeting, see if they would like an update briefing.

Invite the elected official(s) to attend your Planning Meetings and Operational Briefings. We do not operate in secrecy; invite them and assign a knowledgeable staff to escort them through the processes. If they do attend, announce their presence to the group so your folks know who is in the room. If you have a final package of incident maps, damage assessments, rehab plans, team narrative report and the like, have enough packages

developed for presentation to the elected officials who have interfaced with you during the incident.

View the need to meet expectations of citizens and elected officials in the context of these are your "customers." We have a responsibility to meet the expectations of our customers. DO IT! This might place additional demands on the team's time, but we do have a responsibility to keep citizens/elected officials informed. The benefits of expanding this effort will be generally well rewarded. Agency folks left behind after a team mitigates the incident will enjoy an improved respect for the emergency services.

Very Important Persons (VIPs) Visits

Incident visits by interested important people will happen. VIPs could be just about anyone, politicians, government department heads, etc. Be prepared for them! Some will be invited; some will appear unannounced. Regardless, teams should have internal procedures (team guidelines) in-place and known by all members to deal with these important visitors.

A team function should be designated to be responsible for VIPs. Routinely, this falls to the Public Information Officer. However, dependent upon the visitor, an Incident Commander/members of the Unified Command may be expected to make a presentation to the VIP. It really doesn't matter who is responsible for VIPs, but there must be a function responsible and staffed to handle these folks.

The goal in these visits is to brief the VIPs on the incident's history, what is projected and what problems exist. Visual aids in a briefing area will make this much easier. Make sure that you tour incident developed facilities with VIPs in a way that doesn't disturb the work being conducted. Orientations to the Planning Section's efforts will usually amaze folks seeing this activity for the first time. The same is true with the Finance Section. Of course, a tour of facilities isn't complete without trying the kitchen.

You should expect requests for tours to the front lines. If practical, go with appropriately marked PPE and in agency marked vehicles. Expect and plan for over-flight requests; these are appropriate when correctly licensed aircraft are available and such movement does not interfere with operations. Upon departure of the VIP, ask if a follow-up personal briefing is of value for them. A simple phone number exchange will allow rapid transfer of information to them and could limit return visits.

Accountability

Deficiencies in accountability is an often-discussed issue for incidents, but one which can also be difficult to improve. In a team setting, accountability must start with the team. Team guidelines have laid out specific expectations; were they met? Your Agency Administrator laid out expectations (strategic goals and objectives) for the team; were they met? Section Chiefs laid out expectations for their subordinates; were they met? How do you know? We historically have done poorly when recording job performance with proper documentation (refer to Activity Log on page 246). Change this trend!

Performance Issues

Substandard or non-performance is not a frequent occurrence, but one that will need to be addressed when it occurs. If a performance issue negatively impacts the incident, have the appropriate IMT authority release the individual and send them home. Follow this with immediate contact to their home supervisor advising of the situation and the reason for the early return. Follow up with written documentation that includes all pertinent facts. You had better be right as this is about the biggest action you can take against a professional and one that may take follow-up action after the incident. But hey, that's what you get the big money and title for.

Personnel problems must be referred to the Incident Commander at once. Some tough decisions must be made. Is the transgression or act sufficient to warrant future punitive action? If so, recommendation is that a specific investigator for the occurrence be requested. Current personnel assigned to the incident already have a job and/or might not have expertise to perform and document a needed investigation properly. Get specialized help when needed.

To assist in defining standards of conduct, Teams should have established written incident rules of conduct available in their laptop computer. This will need to detail acceptable/unacceptable conduct and attire for personnel to adhere to. Post on bulletin boards and include in IAPs as deemed appropriate. Then BACK IT UP!

Individual and Team Performance Ratings

Team members with written guidelines know what is expected of them. Performance ratings should have these expectations incorporated as rating factors. If met, say so. If not, explain why performance was less than adequate. Improvement for a next deployment is the goal. Refer to ICS Form 225, Incident Personnel Performance Rating, on page 249 and Check Out/Team Evaluations on page 213.

Agency Administrators will often be very satisfied with a team's performance when the incident is successfully controlled; sometimes, to the point of embarrassment. However, do they really review your documentation, ask for final cost figures, demand reviews of accidents and injuries or feel free to discuss on-going political problems in an incident's aftermath? No, but these are the issues that administrators deal with. As a last professional gesture, what would an administrator do with a performance rating sheet listing these types of issues handed to him or her by an Incident Commander? It might be worth doing just that to watch their expression. If you get one honestly filled out, it will make a great learning tool for the entire team.

Section heads must understand it's an obligation of their position to honestly rate subordinates. The team should decide early (in their guidelines) to what level of the organization performance ratings would be required. Once done, make the forms available

and have a central location staffed for their collection. Distribute off the incident under direction of agency policy or the Agency Administrator

Mutual Aid

Your incident may have numerous mutual aid resources. A common situation but one that does have implications associated with it. There should be a required a periodical review and assessment by Operations on the effectiveness and value of these resources. On many occasions, we can look back and confidently say these resources were held too long. These have, at times, become a security blanket in case "something goes wrong." In many cases, their true value ended 24 hours previously. Actively monitor this.

Get the right resource type for your requirement. Why do we continue to associate "structure protection" needs with Type I engines? In many locations, these monsters have limited applications. Nearly as many Type II and III engines are available through the system, and these lend themselves better for many more applications. Think about capabilities and limitations when ordering resources. Demobilizing a large collection of mutual aid resources can become a nightmare. Plan early and staff up. The vehicle safety inspection portion takes a while.

Section 8 - Planning for Demobilization

You have stabilized the incident and begin planning for demobilization. As the primary thrust to accumulate resources was driven by operation's needs, this section has primary responsibility to generate information on their future needs and scale-back of the incident. One tool to assist in this "crystal ball" projecting is a matrix developed by Operations. The matrix (refer to Glide Path on page 204) lists different types of resources to be used, each operational period out for a minimum of three days and projected needs of each type of resource for each subsequent operational period. Operations should review this matrix often. With exception of the following operational period, numbers can be changed as each operational period completes their assignment, and the needs change up or down. Armed with this type of information, the team can begin demobilization planning and proceed. Plan early, review often and demobilize resources that are not needed.

What's Coming Your Way Next?

What is on the horizon for IMTs? Who knows? However, if recent deployments are an indicator of the future, things will be interesting. New challenges exist and possible assignments for situations yet unknown surely will test skills of current and future team members.

The adoption of and enhancements to NIMS and NQS by the Federal government impacts Incident Management Teams. Incident management and coordination have been given additional emphasis, and new tools, guides and systems have been developed to increase national IMT capacity. Availability of trained/experienced IMTs is becoming known by many jurisdictions that previously had very little knowledge of these resources. Most jurisdictions

lack their own IMTs and are trying to train and learn a system that they only exercise occasionally or when "the big one" happens. Many jurisdictions have limited ability to function proficiently due to a lack of resources and of continuous application of these skills. With these specialized skills available on demand in the form of IMTs, many jurisdictions will look to IMTs to fill their occasional needs. What will this entail?

New types of incidents will need to be managed and any location could be impacted. Large-scale HAZMAT, civil disturbances, earthquakes, floods and, yes, an occasional tsunami are potential threats and hazards we face. Who knows what other unforeseen calamity will jolt nature's playground for disasters? Whatever incidents we encounter, however, will require massive amounts of resources for mitigation. Will managing these effectively be that much different than other incidents you are responsible for? No, only the actual application of these resource's skills will be somewhat different. In other words, effectively dealing with large numbers is not any bigger deal than what we routinely do; only the application will differ. What can a team expect?

IMTs will not normally have knowledge or training in many areas needed when dealing with large numbers of displaced citizens (both short and long-term), addressing water and air pollution concerns on a large scale, restoring basics of life needed to survive like emergency drinking water systems and food as well as many other aspects. To assist in getting these tasks completed, get the most knowledgeable technical specialist for areas where the corporate knowledge of the team is lacking and then listen to them! Developing interpersonal skills that will be necessary to coordinate and interact with personnel from many diverse agencies and jurisdictions. This is not as easily done as you might think. You will have inherent problems with some because of the "What do a bunch of wildland firefighters know" syndrome. You will not have that warm fuzzy feeling that you have done this incident a hundred times to fall back on. However, you will have tested emergency management skills exceeding those around you. The pressure to perform without a hitch will be ever present. This could be voiced or personally felt by individual team members. Effects might become overwhelming. Teams should discuss this and recognize its symptoms. You will need to consider concerns for team member's personal property and family could surface. Were member's residences within an affected area? This should be dealt with this straight away. And the expenditure of dollars will be a nagging hindrance to feeling free to do what is needed. "Where is all of this money coming from" will become a steady nightmare.

With new types of incidents will come new types of assignments. You might not oversee the big picture; a part or role could have been delegated (e.g., managing the receipt and distribution of relief supplies, restoration of water supplies). You could be working for another management organization (team) on a portion of the overall incident that may or may not be experienced/knowledgeable.

EOCS

With expansion of emergency response coordination under NIMS comes new guidance and tools for EOCs at various levels of government. Training is expanding for EOC personnel. A challenge is that many EOC staff perform EOC duties as an added responsibility to their normal job. Many have only limited knowledge of performing in an emergency response mode. Fewer have performed on emergency incidents. We can anticipate that many agencies will look to IMTs for assistance. IMTs bring known capabilities and increasingly are being utilized in EOC roles throughout the states. This knowledge is being shared and expanded within those circles. What will a team face while filling a request to function within an EOC (refer to page 30)?

- A clear delegation of roles and authorities will be needed. This should be a must even if the team has to help in developing them (and you should/will). You could be working in an arena without benefit of legal backing; may not be legislated to do some of the roles as expected on wildland fires. Get your delegation right and in enough detail to cover you and the agencies you represent.
- A team could be delegated to act as the sole management representative of the responsible jurisdiction. Delegation would need to be very specific and complete. Ramifications from an indiscriminate delegation could become monumental. This could equate to being delegated responsibility for a fire emergency.
- A team could be requested to perform as “shadows” or deputies within an EOC with responsible jurisdiction personnel filling all “lead” roles. The easiest way to visualize this scenario is a team would be performing a “training” mission of walking the other personnel through the para-military organization of ICS and developing team building skills of the personnel. True delegation of authority would never leave the jurisdiction, but a team will need clear definition of their expected role.
- A team could be delegated part(s) of large incidents to manage. Again, very specific delegations would need to be documented.

CONCLUSION

So that’s the whole picture as the authors see it. The intent of this article was to afford you some “words of wisdom” from experienced/knowledgeable folks. It is hoped that as you encounter new challenges as a member of an IMT, that you will be able to draw from this information in determining your approach incidents.

Appendix F Annex 1 - Example of IMT Standard Operating Guidelines

2021

Example Standard Operating Guidelines

Editor's Note: Thank You to California Interagency IMT 4 – Rocky Opliger (IC) for input on this document

Incident Commander's Intent

This Standard Operating Guide (SOG) provides information and clarification to team members on how the team will function to accomplish specific tasks and goals when assigned to an incident. This SOG is an internal document.

These agreements and guidelines were developed over time by IMT members to address issues not found in other guiding documents such as job aids and position checklists; or to cover unusual situations where guiding documents are unclear or conflict with one another.

These SOGs are guidelines and should be used appropriately. The guidelines are a place to start solutions, not necessarily finish. Each incident is different and may require a different approach to overcome obstacles or take advantage of opportunities. I expect all of you to work together and create the most appropriate solution.

Other Team-Specific Documents Used by IMT

There are two other guiding documents used by this IMT that should not be confused with this SOG.

Team Member Expectations This document describes my expectations of all personnel who accept an assignment as members of this IMT. It discusses team norms and lays out expected behaviors for all of us to work together as a team. This document is intended for our IMT members as an internal document.

Expectations This document outlines administrative procedures and direction on behavior and conduct for all resources assigned to an incident. It will be distributed to each resource leader as they check-in to the incident. Division/Group Supervisors will ensure each module has received the document.

Standard Operating Guidelines (SOGs)

The following SOGs are not listed by Section or function. This is intentional as most items are cross functional. As such, they are listed by topic or activity.

Incident meetings

There are four types of routine meetings during an incident, in addition to the normal planning process meetings.

1. **Command and General Staff Meeting:** The C&G will meet for lunch and business for approximately one hour from 1200-1300. Attendance is mandatory, and each Section must have a representative. If the primary Command or General Staff member cannot attend the meeting, an alternate will be assigned.
2. **Closed team meetings:** Situations arise when the IC may decide to conduct a special meeting with the C&G or the entire IMT. The IC will set up the time and assign a facilitator.
3. **Cooperator's Meeting:** This meeting is facilitated by the Liaison Officer (LOFR) and supported by the C&G as determined by the LOFR. The purpose is to present intelligence catered to stakeholders, provide them a venue to make their needs known, and coordinate their activities with Operations or other sections as needed. In addition, it provides a venue for the Agency Administrator and the Team to build relationships. Timing needs to be coordinated with the Operations and Planning sections. However, between 0800 and 0900 usually works best with a 12-hour planning cycle.
4. **After Action Review:** IMT will meet for a closed team meeting to conduct an After-Action Review (AAR) at the end of each assignment. Unresolved lessons learned from earlier assignments will be included until completed. Each function shall create an action plan addressing new lessons learned. Lessons learned will be reviewed at the beginning of each assignment.

Medical Unit

The Medical Unit will be in an area that is accessible to the firefighters whenever possible. "Choke points" or heavy foot traffic areas in the base are good locations. In any event, close coordination with the proper unit leaders is essential.

Emergency Medical Evacuation of Injured Responders

The MEDL and OSC will include input from their field personnel when developing the incident-specific medical evacuation procedures to assure local and current information is incorporated into the Medical Plan. The MEDL will meet daily with the COMM Unit to review emergency procedures.

A declared major medical emergency would be handled under the MEDL with direct contact with Safety, OSC and notifications to the IC and other pertinent personnel on the incident. The MEDL will outline procedures that will be used to supply medical help and evacuation of seriously injured responders. Every case is different so the information should be viewed as a framework as per the incidents medical ICS 206, Medical Plan. Actions will be based on best available options at that time. Agency Administrator and any other entities will be notified through the SOF1

Accidents Not Associated with the Incident

The local 911 emergency protocol will be used, and MEDL will help if needed and available. The IC shall be notified if as needed.

Incident within an Incident (IWI)

The Safety Officer (SOF1) is the IWI team lead. At the beginning of each incident, the SOF1 will develop the IWI contact list. At least one test of the notification systems shall be performed within the first 24 hours of assuming command of an incident.

Location of PIO work area

The media and public information area should be found near the front of the base and be clearly identifiable by people entering the base. Secondary consideration is for the PIO to have easy access to the OSC to keep abreast of the latest information and activity occurring on the incident.

Area for media and public information should be found near the entrance to the Base. The PIO office should be in the ICP near the other Command and General Staff.

Significant Event Notification to IC and PIO

Significant events in any function need to be reported to the IC and PIO as soon as practical to prevent rumors and inaccurate information being released to the media or public.

Broadcasting Critical Weather Updates

The PSC/SITL shall watch the weather conditions throughout the day, as well as produce the normal weather forecast. They are expected to make a brief announcement on the Command net when a weather severity threshold has been achieved or a major change in conditions has been observed. Positive Check-back from the OPBD's and DIVS's is needed. Sufficient time must be given to allow for all incident personnel to adjust their assignment appropriately and/or seek shelter.

The weather event must be a departure from earlier expectations or a clear threat to incident personnel. The C&G will be advised of the pending condition prior to the broadcast or as soon as practical.

Work/Rest and personnel/equipment timekeeping

The 2:1 Work/Rest ratio shall be strictly adhered to as described in the Incident Business Management Handbook, MOB Guide and in compliance with the NWCG guidelines memo. All resources working for this IMT will keep detailed records of their hours worked for work/rest ratio tracking purposes. Working over 16 hours must be coordinated and approved in advance by the IC or Deputy IC outside of Operations. When it does occur, the Work/Rest justification/mitigation measures form must be completed, approved by IC, and filed in the Time Unit. Working 16 hours every day should not be the normal practice.

The Crew Time Report (CTR) will be the primary form used to track **personnel** hours worked, but forms from other agencies that track hours worked may be accepted by the FSC. **Performance will be documented daily on each CTR in the Remarks box as "Performance**

Acceptable," or "See Documentation." If there are challenges with conduct or performance, corresponding documentation must be completed.

The Equipment Time Shift Ticket will be used to track **equipment** and is to be signed by the government representative managing the equipment. Pink and Blue copies are to be retrieved by the government representative managing the equipment and turned into Finance DAILY. **Performance will be documented daily on each Shift Ticket in the Remarks box as "Performance Acceptable," or "See Documentation" if there are challenges with conduct or performance** corresponding documentation must be completed.

Recycling

The Logistics Section coordinates recycling with the local officials and follows the protocols of the local area. At times recycling is done at the land fill and it may appear at the base that recycling is not occurring. Team members may obtain information about incident recycling from the Facilities Unit Leader.

Enhancing Communications at Helibases and Helispots

The COML will provide communications input when locations are being considered to provide the best possible communications with helicopter facilities.

Enhanced Resource information on IAPs

"Last days" is a way of Rest Cycle Management of personnel, O (Overhead) numbers and E (Equipment) Resource numbers will be displayed for each resource on the IAP.

Operational Briefings

Operational Briefings will be supplied for all tactical resources and anyone who is going to the field such as EMTs, etc. When tactical resources cannot report to the ICP for the briefing, The IMT will conduct remote briefings and, whenever possible, they will be attended by designated members of the C&G. Contract resources must attend daily operational briefings.

The standard ICS briefing agenda format shall be used with the following emphasis areas:

- Roll call in the large group will include Branch Directors and Division/Group Supervisors. The tactical roll call will be done at the division breakouts and the results reported to the OSC and RESL.
- OPBDs and DIVSs shall be in the front of the crowd, usually stage left, so they can raise their hands and be easily identified by the others.
- The PSC shall ensure every speaker is using the microphone correctly or speaking loudly so they can be heard, this is critical.
- The PSC shall coach non-team members on proper briefing techniques such as not saying things others will say later, don't repeat information, stick to the topic, keep it short, but provide pertinent, quality information.
- Personnel should reference page number in the IAP for assigned topic.

- If team members don't have important things to say they should not speak, or they may tell the PSC to deliver the short information.
- The IC should be the LAST WORD in the briefing. All other information should be delivered before the IC. After the IC gives the closing remarks the PSC should announce that the briefing is concluded.
- Prior to the Operational Briefing the PSC will have everyone who is going to speak stand next to the stage ready to quickly step up. This will save time.
- The briefing order will be posted in a location visible to speakers to remind them when to step forward.
- Discussions about non tactical issues are allowed but must be kept to a minimum and should not distract from the delivery of the operational information.

Early Implementation of eI-Suite

The PSC, CTSP and FSC should work together to implement eI-Suite (Resource Management Tool) upon arrival at an incident to quickly gain control of resource tracking, IAP production and cost tracking. An early ROSS download is essential. Representatives will meet after the in-brief to decide protocols and implementation.

Decision Point for Implementation of Satellite Based Internet Provider

The COML will figure out how long it may take to receive sufficient communication lines to allow internet connection upon arrival at an incident. A satellite internet provider will be deployed if expected to take longer than 48 hours of the in-briefing. Those with absolute need to access the internet can do so from a remote location or "jet pack" to meet interim needs.

Appendix F Annex 2 - Example of a Statement of Incident Commander Expectations

2021 Incident Commander - Expectations

Editor's Note: Thank You to California Interagency IMT 4 – Rocky Opliger (IC) for input on this document

Welcome to this Incident – Thank You for your Cooperation & Support!

CONDUCT AND BEHAVIOR

This team is committed to **"ZERO TOLERANCE"** of careless, illegal, inappropriate, and unsafe actions.

Alcohol and/or illegal drugs: Are **NOT allowed** within the incident environment or while actively assigned to the incident. Local Law Enforcement Officials will be called to deal with any suspected illegal activities. Each employee has the responsibility to be ready, willing, and able to perform the duties for which they are qualified.

Sexual Harassment: Inappropriate actions or comments will not be tolerated. Everyone is expected to act in a professional manner. It is your responsibility to stop inappropriate actions or comments at once upon becoming aware of such. Sexual Harassment must be reported to the Human Resource Specialist or Incident Commander. When outside of your designated sleeping area, you must wear at least a shirt, proper shorts, and shoes or sandals. If you need clarification of these expectations contact the Human Resource Specialist or IC. What we PERMIT we PROMOTE!!!!

SAFETY: The commitment to and accountability for safety is a joint responsibility of firefighters, managers, and administrators. Individuals must personally be committed and responsible for their own performance and accountability. Everyone assigned to this incident can expect an assignment that follows all safety rules & regulations. Every person is expected to always perform his or her duties in compliance with all known safety practices. Anything less is unacceptable.

EMPHASIS AREAS:

Training

All trainees and trainers are expected to follow the procedures outlined in the Training Expectations (note: this is a separate attachment to the source document that has not been included in this annex).

Evaluations

All supervisory personnel assigned will complete an ICS 225 Incident Personnel Performance Rating form for their assigned resources according to agency policy or contractual agreement.

Injuries/Claims

Ensure all injuries and potential claims are reported to the Comp/Claims Unit for completion of paperwork. Contract claims will be reported to the Procurement Unit Leader.

Work Rest Cycles

The 2:1 work/rest ratio is mandatory. For every two hours on shift, you will have to rest for one hour. Every effort shall be used to limit work hours to a maximum of 16. If circumstances require you to exceed 16 hours, this needs to be coordinated in advance with your supervisor and the Justification/Mitigation form completed to support the excessive hours prior to sending for approval by the IC. It is your responsibility to follow this direction and supply the proper documentation to your Supervisor and Finance.

Position Qualifications

Personnel shall only be assigned to positions for which they are qualified. Proof of qualifications shall be approved prior to being assigned to any fire line position. Non-fireline positions may be filled based on the word of the employee pending home unit confirmation, which must be requested at once.

Debriefing

All Branch Directors/Division/Group Supervisors will report to their Supervisor and Situation Unit at the end of the operational period for debriefing with emphasis on the accomplishment of objectives. All unit logs (ICS 214) will be turned in after the debriefing to Documentation reflecting accomplishment and/or special incidents that occurred during the operational period.

Crew Time Reports/Shift Tickets

It is your responsibility to ensure all time is properly accounted for and recorded each shift. The records are to be reviewed and signed by the next level supervisor. A finance "Rules of Engagement" document will be provided in the IAP explaining further requirements.

Social Media

It is your responsibility to know and understand guidelines for firefighter photography, video, and social media use. The IMT's goal is simple: to take part online in a respectful, relevant way that protects our incident's professional reputation, does not confuse the public about the incident and follows the letter and spirit of the law. Be mindful that social media postings can be viewed as unprofessional, damage careers and lead to disciplinary actions. For further information, contact the Public Information Officer.

We look forward to working with you as a valuable member of this effort. If you have any questions or feedback, please feel free to contact any Command and General Staff Member.

_____

Incident Commander

THANK YOU FOR YOUR COOPERATION AND GOOD WORK!!