National Incident Management System

Intelligence/Investigations Function Guidance

February 2025

FEMA

This page intentionally left blank

Table of Contents

Intelligence/Investigations Fundamentals and Concepts in NIMS

The National Incident Management System (NIMS) represents a core set of doctrine, concepts, principles, terminology, and organizational processes enabling effective, efficient, and collaborative incident management. The Incident Command System (ICS), as a component of NIMS, establishes a consistent operational framework that enables government, private sector, and Nongovernmental Organizations (NGO) to work together to manage incidents, regardless of cause, size, location, or complexity. This consistency provides the foundation for the use of ICS for all incidents, from daily occurrences to events requiring a coordinated federal response.

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 shooter incidents, terrorist attacks, or other incidents causing mass injuries or fatalities—require an intelligence or investigative component to determine the cause and origin and/or to support incident/disaster operations.

Intelligence and Investigations (I/I) is one of six major functional areas of the ICS. The scalability and flexibility of NIMS allows the I/I function to be seamlessly integrated with the other ICS functions. The I/I 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, regardless of source. If the incident is determined to be a criminal event, the I/I function leads to the identification, apprehension, and prosecution of the perpetrator. The I/I function can be used for planned events as well as incidents.

1. Introduction

NIMS provides 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[1] with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System.[2]
- A consistent foundation for managing all incidents, from daily occurrences to incidents requiring a coordinated federal response across all mission areas.
- Guidance to apply and implement NIMS components—specifically, Resource Management, Command and Coordination, and Communications and Information Management—in accordance with the NIMS guiding principles of flexibility, standardization, and unity of effort. NIMS is more than ICS and command and control. NIMS is a set of concepts and principles for all threats, hazards, and events across all National Preparedness System mission areas—Prevention, Protection, Mitigation, Response, and Recovery. NIMS ensures consistency and *unity of effort* across mission areas and whole community stakeholders.

Intelligence and Information Sharing is a core capability of the National Preparedness System, covering both the Prevention and Protection mission areas. The NIMS I/I function ensures that intelligence and investigative operations and activities are managed and coordinated to:[3]

- 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, analyze, and store evidence or specimens.
- Conduct thorough and comprehensive investigations that lead to the perpetrators' identification, apprehension, and successful prosecution.
- Conduct missing persons and mass fatality/death investigations.
- Inform and support life safety operations, including the safety and security of all response personnel, by helping to prevent future attacks or escalated impacts.

[1] *Whole community* focuses on enabling the participation in incident management activities of a wider range of players from the private and nonprofit sectors, including NGOs and the general public, in conjunction with participants from all levels of government, to foster better coordination and working relationships.

[2] The National Preparedness System outlines an organized process to help the whole community achieve the NPG. It comprises and builds on existing policies, programs, and guidance, including the National Planning Frameworks, Federal Interagency Operational Plans, and the National Preparedness Report.

[3] FEMA, National Incident Management System, October 2017.

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

NIMS includes flexible options for the incorporation of the I/I function to ensure coordination across all mission areas and core capabilities. This updated NIMS Intelligence/Investigations Function Guidance document provides comprehensive guidance for I/I considerations across all components of NIMS, including Resource Management, Communications and Information Management, and all elements of NIMS Command and Coordination, including guidance for emergency operations centers (EOC), Multiagency Coordination Groups (MAC Groups), and the Joint Information System (JIS), in addition to ICS.

It further provides guidance for coordinating I/I functions across National Preparedness System mission areas to ensure unity of effort and alignment with the National Preparedness Goal (NPG).[4] This includes the relationship between the core capability of Intelligence and Information Sharing and other core capabilities, including Operational Coordination.

2. Applicability and Scope

NIMS applies to all stakeholders with incident management and support responsibilities. The audience for NIMS includes emergency responders and other emergency management personnel, NGOs, the private sector, and elected and appointed officials responsible for making decisions regarding incidents.

While the Intelligence and Information Sharing core capability may be aligned with the Prevention and Protection mission areas, I/I considerations exist in all mission areas under the National Preparedness System. NIMS I/I guidance is intended for all personnel, regardless of discipline, jurisdiction, organization, or mission area, who are responsible for managing efforts to prevent, protect against, mitigate, respond to, or recover from the effects of an incident, regardless of the cause, size, location, or complexity—particularly in situations where sensitive intelligence or investigative tactical operations, resource management, communications, operational planning, information management, and operational coordination must occur to ensure unity of effort and the security and resiliency of the nation. The audience for this guidance includes, but is not limited to, law enforcement and public safety, investigative, emergency management, information management and fusion center, or other Prevention and Protection mission area personnel.

[4] FEMA, National Incident Management System, October 2017.

3. NIMS Guiding Principles Related to Intelligence/Investigations Function

NIMS outlines three guiding principles for applying and implementing NIMS components: flexibility, standardization, and unity of effort.

Flexibility: NIMS components, including the I/I function, are adaptable to any situation, from planned special events to routine local incidents to complex national-level incidents with intelligence or investigative requirements. The NIMS I/I guidance adheres to this principle, offering options for implementing I/I concepts in a flexible, scalable, and modular manner consistent with the needs of the incident.

Standardization: Standardization is essential to interoperability among multiple organizations in incident response and management. NIMS defines standard concepts, practices, systems, organizational structures, and processes that improve integration and connectivity among jurisdictions and organizations and facilitate operational coordination and information management across all mission areas. While adhering to the principle of flexibility, the NIMS I/I function relies on standardization to allow I/I personnel to work seamlessly and effectively across mission areas and within all components of NIMS, fostering cohesion among stakeholders and organizations.

Unity of effort: Unity of effort involves coordinating activities across mission areas and core capabilities and among various organizations and coordinating structures to achieve common objectives, maintain situational awareness, and support the NPG ("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"). By implementing and applying NIMS I/I concepts—in alignment with the Operational Coordination core capability and integrated throughout coordinating structures—leaders can establish and maintain a unified, coordinated operational structure and process that appropriately integrates all critical stakeholders.

4. Background

NIMS is the culmination of more than 40 years of efforts to improve interoperability in incident management. This work began in the 1970s with local, state, and federal agencies collaborating to create a system called Firefighting Resources of California Organized for Potential Emergencies (FIRESCOPE). While the original intent was to establish a system to manage wildland fire field activities, the design intent of the system immediately evolved into an all-risk, all-hazards system; the focus shifted to developing a system to manage an incident of any kind, not just a fire. As a field-level system for applying tactical resources on scene, ICS was identified as a set of best practices. Adoption throughout the fire service and all-hazards response community ensued over the next two decades.

Following the 2001 terrorist attacks, the enactment of the Homeland Security Act of 2002, and the issuance of Homeland Security Presidential Directive 5 (HSPD-5), the Department of Homeland

Security (DHS) was directed to establish a national incident management system enabling all stakeholders to work together effectively and efficiently. DHS and FEMA subsequently led a national effort to identify incident management best practices. This resulted in consolidation, expansion, and enhancement of the FIRESCOPE efforts, as well as other innovations from early adopters and stakeholders, as a comprehensive national system developed.

ICS became a cornerstone of NIMS. Until 2004 (and the release of NIMS), ICS was organized around five functional areas: Command, Operations, Planning, Logistics, and Finance/Administration.[5] In recognition of the post-9/11 environment, leaders were asked to outline ways to incorporate an "Information and Intelligence" function within ICS. Resulting options included establishing this function as part of the Command Staff, as a unit within the Planning Section, as a component of the Operations Section (branch, division/group, strike team/task force, or single resource), or as a sixth function of ICS: a separate General Staff Section.

Information and Intelligence Management was introduced in 2004 as a NIMS/ICS management characteristic, contributing to the strength and efficiency of the overall system. Guidance stated that *the incident management organization must establish a process for gathering, sharing, and managing incident-related information and intelligence.* The analysis and sharing of information and intelligence are important elements of ICS.

The updated NIMS document in 2008 rebranded Information and Intelligence as the Intelligence/Investigations (I/I) function, keeping the previously identified ICS organizational options. In 2013, FEMA released the NIMS Intelligence/Investigations Function Guidance and Field Operations Guide to provide "guidance on how various disciplines can use and integrate the I/I function while adhering to NIMS concepts and principles," with a specific focus on I/I application within NIMS Command and Coordination under ICS.

In 2011, Presidential Policy Directive/PPD-8: National Preparedness was issued to develop a:

- National Preparedness Goal (NPG) to identify the core capabilities necessary for preparedness.
- National Preparedness System to guide activities to enable the nation to achieve the goal.

PPD-8 complements HSPD-5 and NIMS while further associating the NIMS function of Intelligence and Investigations with specific mission areas, notably Prevention and Protection.[6] Regardless, NIMS

[5] ICS is still organized around these five functional areas with the option for I/I to be integrated into the traditional ICS organization (Command and General Staff functions) or as a sixth functional area under an I/I General Staff Section Chief.

[6] In addition to the core capability of Intelligence and Information Sharing associated with the Prevention and Protection mission areas, the following I/I-related core capabilities were identified: Interdiction and Disruption (Prevention and Protection); Screening, Search, and Detection (Prevention and Protection); Forensics and Attribution (Prevention); Access Control and Identify Verification (Prevention); Cybersecurity (Prevention); and Physical Protective Measures (Prevention).

applies across all mission areas—including NIMS guiding principles, fundamental concepts, vocabulary and definitions, systems, and processes—to successfully deliver the capabilities described in the National Preparedness System.[7]

5. Key Terms

Several key terms are used throughout this document. In addition, you can find additional terms in Appendix D and in the NIMS document.[8]

6. Integrating Intelligence/Investigations Functions with NIMS

I/I functions take place during normal operating times (steady state) and during incidents and emergencies. Steady-state I/I functions, including routine operations and information management, are conducted according to established procedures, often in a collaborative, multiagency process. These steady-state efforts may be aligned with the National Preparedness System's Prevention and Protection mission areas.

Successful integration of the I/I function with NIMS requires balancing steady-state I/I with the incident management I/I needs. As steady-state I/I functions evolve in complexity and shift toward actionable intelligence or imminent threat—or lead to a potential or actual incident or emergency—emergency managers and their I/I counterparts must consider the most effective way to integrate I/I functions with NIMS processes and organizational structures based on the specific needs of the incident. A flexible, scalable, and adaptable approach consistent with NIMS principles, concepts, terminology, systems, organizational structures, and processes is needed to enable partners across the nation to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents.

Effective integration of steady-state I/I functions with NIMS incident management concepts—Resource Management, Command and Coordination, and Communications and Information Management—begins with aligning and integrating information and communications management systems and methods to ensure:

- An integrated process for managing the timely flow of information and intelligence across all applicable stakeholders and entities.
- A comprehensive Common Operating Picture (COP) with essential elements of I/I information.

[7] FEMA, National Incident Management System, October 2017.

[8] FEMA, National Incident Management System, October 2017.

- Potential and emerging threat-related circumstances are considered and addressed.
- Incident personnel and other decisions makers have the means and information to make and communicate timely and coordinated decisions informed by relevant I/I information.
- Unity of effort among various organizations to achieve common objectives.
- A thorough and comprehensive investigation, when applicable, leading to the identification, apprehension, and prosecution of perpetrators.

7. Relationship to Other Documents

Three core capabilities of the National Preparedness System—Planning, Public Information and Warning, and Operational Coordination—span all five mission areas and support the execution of the remaining core capabilities. They serve to unify the mission areas and, in many ways, are necessary for the successful execution of all core capabilities. Specifically, Operational Coordination serves to establish and maintain a unified and coordinated operational structure and process that integrates all critical stakeholders, including coordinating structures, across mission areas.

NIMS guides all levels of government, 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.

The National Preparedness System identifies Intelligence and Information Sharing as a core capability within the Prevention and Protection mission areas. The Intelligence and Information Sharing core capability is described as follows:

> *Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs [weapons of mass destruction]; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.*

Additionally, Information and Intelligence Management is identified as a foundational characteristic of NIMS Command and Coordination, contributing to the strength and efficiency of NIMS. As a NIMS management characteristic, Information and Intelligence Management is described as follows:

> *The incident management organization establishes a process for gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence. Information and intelligence management includes identifying essential elements of information (EEI) to ensure*

personnel gather the most accurate and appropriate data, translate it into useful information, and communicate it with appropriate personnel.

Besides Intelligence and Information Sharing, other National Preparedness System core capabilities with links to the NIMS I/I function include the following:

- **Interdiction and Disruption:** Delay, divert, intercept, halt, apprehend, or secure threats and/or hazards.
- **Screening, Search, and Detection:** Identify, discover, or locate threats and hazards through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, bio surveillance, sensor technologies, or physical investigation and intelligence.
- **Forensics and Attribution:** Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source. This may include attribution for an attack and for the preparation for an attack in an effort to prevent initial or follow-on acts or swiftly develop counter-options.

In summary, by using NIMS, the core capability of Operational Coordination, and the coordinating structures described in the National Preparedness Frameworks and Federal Interagency Operational Plans (FIOP), we as a nation can establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities across all mission areas—including simultaneous execution of independent but related core capabilities and operations—to ensure the security and resilience of the United States in response to threats such as terrorism, cyberattacks, pandemics, and catastrophic natural disasters.

8. Supersession

This document supersedes the NIMS Intelligence/Investigations Function Guidance and Field Operations Guide document issued October 2013.

Intelligence/Investigations Resource Management

NIMS Resource Management guidance enables various organizational elements to collaborate and coordinate to systematically manage resources—personnel, teams, facilities, equipment, and supplies. Most jurisdictions and organizations do not own and maintain all the resources necessary to address all potential threats and hazards. Therefore, effective resource management includes leveraging each jurisdiction's resources, engaging private sector resources, involving volunteer organizations, and encouraging further development of mutual aid agreements.[9]

NIMS Resource Management includes resource management preparedness, resource management during an incident, and mutual aid. See the NIMS document for more information.[10]

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

Resource management during an incident includes standard methods to identify, order, mobilize, and track resources.

Mutual aid, which occurs routinely to meet the resource needs identified by the requesting organization, involves sharing resources and services between jurisdictions or organizations.

1. Identifying and Typing Resources

Resource typing is defining and categorizing incident resources by capability. Resource typing definitions establish a common language for discussing resources by defining minimum capabilities for personnel, teams, facilities, equipment, and supplies.

The following Intelligence and Information Sharing core capability resources are typed under NIMS and published in the Resource Typing Library Tool (RTLT):

- Fusion Liaison Officer.
- Intelligence Analyst.

[9] FEMA, National Incident Management System, October 2017.

[10] FEMA, National Incident Management System, October 2017.

- Intelligence Group Supervisor.
- I/I Section Chief.
- Investigative Operations Group Supervisor.[11]

Resource Typing Library Tool

RTLT is an online catalog of NIMS resource typing definitions and job titles/position qualifications. The RTLT, found at www.fema.gov/resource-management-mutual-aid, lets users search by resource type, discipline, core capability, or keyword.

2. Qualifying, Certifying, and Credentialing

The Authority Having Jurisdiction (AHJ) qualifies, certifies, and credentials NIMS positions.[12] Tools to help with this process include several Intelligence and Information Sharing core capability resources typed under NIMS and published in the RTLT. In addition, the NIMS Intelligence Group Supervisor, I/I Section Chief, and Investigative Operations Group Supervisor resources are included in the National Qualification System (NQS), with Position Task Books (PTB) to document the successful completion of tasks specific to the position. Yet, AHJs have identified numerous I/I positions/functions that would participate in an I/I incident but are not listed in the RTLT or NQS. The Incident Commander (IC)/Unified Command (UC) determines how best to use these responders.

3. Planning for Resources

Resource Management personnel should consider resources necessary to support all mission areas. In doing so, they should consider how multifunction I/I resources (that is, I/I resources that serve a dual purpose and may be tasked with another function, such as Emergency Medical Services (EMS), incident management, law enforcement operations, on-scene security, mass care, or search and rescue) may be used in all-hazards incidents that span multiple mission areas. For example:

- Will multifunction I/I resources be prioritized for non-I/I tasks?
- Will traditional I/I resources be repurposed based on incident priorities?
- Can I/I resources be requested from other agencies and jurisdictions via mutual aid?

[11] Intelligence Group Supervisor, Intelligence/Investigations Section Chief, and Investigative Operations Group Supervisor resources are included in the NQS and have PTBs to document the successful completion of tasks specific to the position.

[12] FEMA, National Incident Management System, October 2017.

- What are the essential I/I tasks that need to be staffed?
- Can non-I/I resources receive just-in-time training to augment I/I functions?

4. Mutual Aid

Jurisdictions and organizations frequently share or exchange I/I information, services, and resources through mutual aid agreements and compacts. Using resource typing and industry standard qualification, certification, and credentialing processes will ensure consistency and facilitate interoperability among I/I resources drawn from multiple jurisdictions or organizations. When I/I resources are exchanged through mutual aid, processes should be in place to verify and validate an individual's clearance level and need to know sensitive information.

I/I resources, including Fusion Center Liaisons and Intelligence Analysts, may be exchanged between various jurisdictions or organizations, including NIMS Command and Coordination entities (Incident Command Posts [ICP], EOCs, MAC Groups, etc.), to facilitate I/I information exchange and coordination and augment operations. Leaders should include the details of potential resource exchanges in mutual aid agreements, Memorandums of Understanding (MOU), standard operating procedures, standard operating guides, and Emergency Operations Plans (EOP). Documentation may include processes to:

- Identify resource and information requirements.
- Request, mobilize, and assign resources.
- Confirm certifications, qualifications, credentials, and clearance levels.
- Report and exchange I/I-related information.
- Organize resources for incident assignment (single resources, strike teams or resource teams, and task forces).

The NIMS concepts of sharing information to inform a comprehensive COP, multiagency coordination, decision-making, and unity of effort need to be balanced with I/I requirements—including legal, policy, operational security, and strategic requirements—to ensure overall public safety. Many federal, state, and local agencies do not accept clearance from other AHJs when sharing law enforcement sensitive information and intelligence with all-hazards partners (emergency management, fire, public health, public works, private sector, etc.) and the whole community. Access to certain restricted or classified information depends on applicable law and policy, as well as an individual's security clearance and need to know. AHJs must address these details before an incident to improve information sharing, ensure overall public safety, and quickly address the incident.

Command and Coordination

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

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

1. Tactical activities to apply resources on scene.
2. Incident support, typically conducted at EOCs, through operational and strategic coordination, resource acquisition and information gathering, analysis, and sharing.[13]
3. Policy guidance and senior-level decision-making.
4. Outreach and communication with the media and public to keep them informed about the incident.

These four areas may be coordinated through the various NIMS functional groups: ICS, EOCs, MAC Groups, and JIS. The Command and Coordination component describes these structures and explains how various elements operating at different levels of incident management interface with one another. By describing unified doctrine with common terminology, organizational structures, and operational protocols, NIMS enables everyone involved in an incident—from the IC at the scene to national leaders in a major disaster—to harmonize and maximize the effects of their efforts.

1. NIMS Management Characteristics

NIMS management characteristics provide the foundation for incident command and coordination under NIMS and contribute to the strength and efficiency of the overall system.[14]

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

[14] FEMA, National Incident Management System, October 2017.

2. Incident Command System

ICS is 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 specifies an organizational structure for incident management that integrates and coordinates a combination of procedures, personnel, equipment, facilities, and communications. Using ICS for every incident helps hone and maintain skills needed to coordinate efforts effectively.

ICS is used by all levels of government as well as by many NGOs and private sector organizations. ICS applies across disciplines and enables incident managers from different organizations to work together seamlessly. This system includes five major functional areas, staffed as needed for a given incident: Command, Operations, Planning, Logistics, and Finance/Administration.[15]

The mission of the I/I function is to ensure that all I/I operations and activities are managed, coordinated, and directed in order to:

- Prevent, protect against, mitigate, respond to, or recover from the effects of potential unlawful activity, incidents, and/or attacks.
- Collect, process, analyze, secure, and appropriately disseminate information and intelligence.
- Identify, document, process, collect, create a chain of custody for, safeguard, examine, analyze, and store probative evidence.
- Conduct a thorough and comprehensive investigation that leads to the identification, apprehension, and prosecution of the perpetrators.
- Serve as a conduit to provide situational awareness (local and national) pertaining to an incident.
- Inform and support life safety operations, including the safety and security of all response personnel.

To accomplish the mission of the I/I function, the IC/UC will determine the incident objectives and strategies and then prioritize them. These priorities may shift as an incident changes. Ultimately, life safety operations are the highest priority, with I/I operations being initiated concurrently. The IC/UC ensures that provisions are made for the safety, health, and security of responders and that I/I operations contribute to a safer, healthier, and more secure life safety operation.

The NIMS Command and Coordination component gives IC/UC several options for establishing the I/I function in a way that meets incident complexity needs. The I/I function may be established in any of

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

the following organizational areas: as a General Staff Section, Command Staff position, within the Planning Section, within the Operations Section, as an EOC function, or wherever appropriate as dictated by the IC/UC.

The nature and specifics of an incident, in addition to legal constraints, could restrict the type and scope of information that may be readily shared. When information affects or threatens life safety of responders or the public, the information can and should be shared with appropriate Command and General Staff. The scalability and flexibility of NIMS seamlessly integrates the I/I function with the other components of ICS.

The I/I function can be integrated into the ICS organization in various ICS positions:

- An Assistant Liaison Officer for I/I which provides input through the Liaison Officer.
- An I/I Technical Specialist (THSP).
- A unit in the Planning Section.
- An I/I group or branch in the Operations Section.
- A separate I/I section.

This scalability and flexibility ensure the I/I function fits NIMS ICS. See Appendix B for further discussion of the options for use of the I/I function in ICS.

3. Emergency Operations Centers

EOCs serve as crucial components in national emergency management, providing a centralized location where multiple agencies converge to address threats and coordinate support for incident command, on-scene teams, and other EOCs. These centers can be permanent, temporary, or virtual, with staff contributions happening on-site or remotely.

Teams operating within EOCs vary in purpose and authority but primarily focus on consolidating and exchanging vital information, supporting decision-making, allocating resources, and maintaining communication with various field personnel. Personnel supported include staff at ICPs, individuals handling tasks not directly affiliated with an ICP, and personnel in different EOCs. The information consolidation work can involve I/I, with EOCs analyzing intelligence reports and ongoing investigations to inform coordinated responses or preempt potential crises.

Additionally, EOC staff often manage specific operations indirectly related to the incident scene, like emergency shelters, especially when no on-scene incident command exists. They might also direct tactical operations during incidents like natural disasters or coordinate efforts across multiple incidents. Occasionally, incident command or Area Command functions are conducted directly within the EOC.

EOCs also activate personnel for prevention, protection tasks, and sourcing backup resources when others are deployed. Key roles within EOCs encompass:

- Gathering, analyzing, and disseminating information, incorporating I/I data to enhance situational awareness and informed decision-making.
- Handling resource logistics, from allocation to tracking.
- Developing coordination strategies and assessing ongoing and future requirements.
- Occasionally offering overarching coordination and policy guidance.

Individual agencies maintain their own Department Operations Centers (DOC) focused on internal activities and asset coordination. While these DOCs engage in external communication and may delegate liaisons, their focus remains on their own operations; this distinguishes them from the inherently multidisciplinary[16] EOCs referenced in NIMS. See the NIMS document for more details on EOC staff structures and procedures for activation and deactivation.[17]

4. Multiagency Coordination Group

MAC Groups, integral components of the off-site incident management structure under NIMS, comprise representatives from various stakeholder agencies or organizations. They come together to make cooperative multiagency decisions, functioning as policy-level bodies during incidents. They are instrumental in resource prioritization and allocation, facilitating decision-making among the officials in charge of the incident, such as the IC. Sometimes EOC staff also participate in these critical activities.

MAC Groups typically include agency administrators and executives or their appointed representatives. They can be established at any organizational level (local, state, tribal, or federal) or across disciplines (emergency management, public health, critical infrastructure, or the private sector). In some localities, legal or policy stipulations might require a MAC Group to sanction additional resources or provide strategic guidance to EOC staff and ICs.

Crucially, MAC Groups do not replace the primary functions of operations, coordination, or dispatch organizations, nor do they perform direct incident command tasks—a role reserved for the UC. They step in for significant resource prioritization and allocation, especially under circumstances of considerable resource contention, thereby assisting coordination and dispatch organizations.

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

[17] FEMA, National Incident Management System, October 2017.

The composition of MAC Groups is strategic. While it often includes directly affected entities or those whose resources are committed to the incident, the inclusion of I/I units is also vital. These units play a crucial role by offering actionable intelligence, supporting informed decision-making, and enhancing overall situational awareness. Additionally, members from nontraditional sectors such as local business or volunteer organizations might not offer tangible resources but contribute through relationships, influence, or specialized knowledge, thereby underpinning the MAC Group's effectiveness in incident response and recovery. MAC Group members are empowered by their respective organizations to allocate resources and funds as needed for incident activities, typically working toward consensus in decisions. Furthermore, the adaptability of MAC Groups allows them to operate virtually, meeting current operational demands efficiently.

5. Joint Information System

JIS is a foundational pillar of I/I function integration within NIMS.[18] JIS ensures the synchronization of public messaging among key structures of incident management: ICS, EOCs, and MAC Groups. It weaves incident information and public affairs into a single, cohesive entity. This integration is pivotal in ensuring that all messaging is consistent, coordinated, accurate, accessible, timely, and complete, particularly during incident operations.

I/I within the JIS framework, when authorized by the IC/UC or designee, allows for:

- **Coordinated intelligence monitoring and sharing:** I/I units, operating within the ICS and NIMS structures, leverage the JIS to circulate authorized vital intelligence as needed, ensuring that all operational decisions are informed by accurate, real-time information. This intelligence is not just confined to internal operations but, as authorized, extends to the public and other stakeholders. A streamlined, coordinated approach is therefore required. To ensure the confidentiality of the investigation, the JIS must receive clear guidance regarding the information that may be released to the media. The JIS should monitor information disseminated by the media, including social media and other relevant sources, and immediately transmit relevant information to the IC/UC or designee.

- **Investigative synergy:** Investigations often provide the context for operational intelligence in incident scenarios. Through JIS, investigative insights are not siloed or isolated in a way that hinders effective communication. Instead, when authorized, insights are immediately shared with the IC/UC or designee and then, if appropriate, shared across agencies and units, reinforcing the intelligence picture and strengthening the collective response to incidents.

- **Operational consistency and message accuracy:** With the backdrop of a unified strategy for public communication, I/I sectors contribute to and draw from a repository of information that maintains the integrity and accuracy of the operational narrative. This approach is essential to

[18] FEMA, National Incident Management System, October 2017.

counteracting misinformation and preserving public trust throughout incident management phases. Authorized information is disseminated to the media only with permission and clear guidance from the IC/UC or designee.

- **Intelligence operations:** I/I branches, via the JIS, engage in a dynamic operational dialogue, remaining responsive to the fluid nature of incident management. The JIS infrastructure is attuned to the nuanced demands of both strategic intelligence and front-line investigation, facilitating a responsive adjustment of public messaging and operational directives.

- **Strategic public communication:** I/I information requires prudent dissemination. The JIS provides a structured avenue for such activity, ensuring that public communications are strategically aligned with intelligence imperatives and sensitive investigative details.

The integration of I/I functions within the JIS marks a strategic confluence of confidential operational details and public communication. This intersection within the NIMS and ICS frameworks underscores the importance of coordinated, accurate messaging in preserving national security and effective incident management. The reciprocal relationship between I/I operations and public information, as facilitated by the JIS, forms a bedrock of trust, compliance, and collaborative efficiency in the face of incidents that require a harmonized multiagency response.

6. Interconnectivity of NIMS Command and Coordination Structures

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

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

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

Communications and Information Management

Effective emergency management and incident response activities rely on flexible communications and information systems to provide a COP to emergency management and response personnel. In planning for communications and information management, leaders should address the policies and procedures, equipment, systems, standards, and training necessary to achieve integrated communications.

Two essentials of a sound I/I function are information management systems and the means necessary to safeguard information—such as information security protocols. Effective information management includes identifying and understanding communications systems, tools, procedures, and methods. Those operating the I/I function should ensure that all necessary types of I/I—including voice, data, image, and text—are shared among appropriate personnel (people with the appropriate clearance, access, and need to know) in an authorized manner—that is, via an appropriate Information Technology (IT) system. They should also work together to protect Personally Identifiable Information (PII), understanding the combinations of laws, regulations, and other mandates under which various local, state, tribal, territorial, insular area, and federal agencies operate.[19]

The NIMS Communications and Information Management component is critical to the I/I function. Implementing processes that foster information sharing while ensuring security of communications, I/I information management requirements, and operational security is essential to the successful integration and implementation of I/I within NIMS.

NIMS Principles of Communications and Information Management

The following principles of communications and information management support incident managers in maintaining a constant flow of information during an incident:

- Interoperability.
- Reliability, scalability, and portability.
- Resilience and redundancy.
- Security.

[19] PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information [2010]).

- Accuracy.
- Timeliness.

Incident personnel rely on flexible communications and information systems to obtain and provide accurate, timely, and relevant information. Establishing and maintaining situational awareness and ensuring accessibility and interoperability are the principal goals of the NIMS Communications and Information Management component. Properly planned, established, and applied communications facilitate consistent information dissemination among all appropriate stakeholders.

The NIMS Communications and Information Management component describes processes and recommended organizational structures to ensure that incident personnel and other decision-makers have the means and information to make and communicate decisions.

A key element of the I/I function—whether it is occurring during steady state or as part of NIMS incident management—is information management. This includes:

- Assessing and defining information requirements.
- Collecting and processing raw information and data.
- Validating and analyzing information.
- Disseminating information, as needed.
- Updating information and reevaluating requirements.

The general processes of NIMS information management as well as I/I-specific information management are similar, with two noted exceptions:

1. Access to and dissemination of I/I information may be limited or restricted to appropriate stakeholders.
2. Certain aspects of I/I information management, such as the collection, processing, validation, and analysis of sensitive information, may occur outside of NIMS structures (i.e., within steady-state I/I processes, systems, and organizations).

Of paramount importance when incorporating I/I functions within NIMS processes and organizational structures is adequately addressing I/I information management requirements.[20] These requirements include:

- Access to and storage of I/I information.

[20] Sensitive intelligence information should be protected by limiting access to those with a need to know.

- Communication and dissemination of I/I information.
- Use and protection of I/I information.
- Designation of the decision-making authority for Priority Information Requirements.

NIMS I/I guidance to date has largely focused on how to organize the I/I function within NIMS Command and Coordination systems, specifically ICS. Though this is an important element of I/I integration within NIMS, it is not the only area of NIMS where I/I needs to be considered. This section will provide guidance on the unique I/I requirements for aligning and integrating with NIMS Communications and Information Management concepts, systems, methods, and processes.

1. Intelligence and Information: Common Terminology and Process

Within the intelligence field, *information* is considered a component of intelligence, especially when referring to raw information in the context of a finished intelligence product. In the incident management field, *intelligence* is considered a component of the overall incident information used to inform a COP. Incident managers recognize that intelligence—or, more broadly, I/I information—may be a protected or restricted subset of incident information, with access limited to authorized decision-makers and responders with a specific need to know.

Information vs. Intelligence

According to *Comprehensive Planning Guide (CPG) 502: Considerations for Fusion Center and EOC Coordination*, information and intelligence (in the context of the intelligence sector) are differentiated as follows:

- **Information:** Pieces of raw, unanalyzed data or reports from various sources about an event, criminal activity or subject of interest.
- **Intelligence:** The product of the collation, evaluation, and analysis of raw information with respect to an identifiable person or group of persons in an effort to anticipate, prevent, or monitor possible threats (i.e., criminal, terrorist or naturally occurring activity).

"Intelligence is information that has been analyzed to determine its meaning and relevance."

Regardless, there is a strong connection between intelligence and information, and there are commonalities between the generic intelligence process[21] by which information is gathered,

[21] INTEL - How the IC Works (intelligence.gov)

assessed, and distributed in the intelligence field and NIMS information management data collection and processing.[22] Table 1 displays these commonalities.

Table 1: Intelligence Process/Cycle vs. NIMS Information Management Data Collection and Processing

Generic Intelligence Process (or Cycle)	NIMS Information Management Data Collection and Processing
1. Planning and Direction	1. Initial Size-Up/Rapid Assessment
2. Collection	2. Data Collection Plans
3. Processing and Exploitation	3. Validation
4. Analysis and Production	4. Analysis
5. Dissemination	5. Dissemination
6. Evaluation	6. Updating

While the processes are similar, the key distinction is that NIMS information management processes assume the goal is interoperability and wide dissemination of incident information, while general I/I processes inherently protect sensitive information and disseminate information through secure channels to stakeholders with a need to know.

These distinctions must be understood when integrating I/I functions with NIMS systems, organizations, and processes and incorporating I/I data into plans and incident-specific procedures and decisions. The NIMS Communications and Information Management component recognizes the need for information/operational security, specifically noting that the need for confidentiality and information protection can complicate information sharing. This can be particularly pronounced when sharing law enforcement sensitive information and intelligence with all-hazards partners (emergency management, fire, public health, public works, private sector, etc.) and the whole community. Access to certain restricted or classified information depends on applicable law and policy, as well as an individual's security clearance and need to know. The NIMS concepts of sharing information to inform a comprehensive COP, multiagency coordination, decision-making, and unity of effort need to be balanced with I/I requirements—including legal, policy, operational security, and strategic—to ensure overall public safety.

[22] FEMA, National Incident Management System, October 2017.

2. Communications Management and Information Management

Coordination is essential for effective and efficient management of any incident or planned event. When specialized resources, such as analysts or investigators, become active during an incident, the need for coordination increases, as other operational activities may conflict with I/I function activities. NIMS provides guidance on communications and information management related to the following topics, discussed in detail below:

- Communications management.
- Incident information.
- Communications standards and formats.

3. Communications Management

NIMS communications management guidance focuses on interoperability and helping incident personnel from different disciplines, jurisdictions, organizations, and agencies communicate with each other effectively during incidents. This principle applies to the I/I function with an additional emphasis on secure communications and protection of I/I-related information. NIMS defines four communication types: strategic, tactical, support, and public.

NIMS Standardized Communication Types

Strategic: High-level directions, including resource priority decisions, roles and responsibilities determinations, and overall incident management courses of action.

Tactical: Communications between on-scene command and tactical personnel, and cooperating agencies and organizations.

Support: Coordination in support of strategic and tactical communications (e.g., communications among hospitals concerning resource ordering, dispatching, and tracking; traffic and public works communications).

Public: Alerts and warnings, press conferences.

I/I communications may span all four communication types. Restricted communications channels should be established as appropriate. This is particularly relevant as it relates to tactical communications involving I/I resources, operations, or information. Outside of secure I/I tactical communications, efforts should be made to share and communicate information as needed, in keeping with I/I information management policies.

The Communications Unit establishes the overall incident communications infrastructure and networks, including voice and data communications and IT systems. I/I personnel can be assigned to the Communications Unit to assist with the management of I/I communications—specifically,

hardware, systems, networks, and infrastructure. This would allow I/I communications to be included in the Communications Unit but managed and protected by I/I personnel. If the I/I communications requirements exceed the ability of the Communications Unit to effectively manage I/I communications, a separate I/I-specific Communications Unit could be established—complete with its own physical protections—to establish and guard sensitive and restricted communications equipment and systems.

3.1. Command and Management

The ICS, Multiagency Coordination Systems (MACS), and public information are the fundamental elements of incident management. These elements provide standardization through consistent terminology and established organizational structures. The collection, analysis, and dissemination of incident-related information and intelligence are aspects of ICS. The I/I function provides several critical benefits to an IC/UC, such as:

- Ensuring that information and intelligence of tactical value is collected, exploited, and disseminated to resolve an imminent threat or prevent an imminent attack or follow-on attacks.
- Ensuring that I/I activities are managed and performed in a coordinated manner to prevent the inadvertent and inappropriate:
    - Creation of multiple, conflicting investigative records.
    - Use of different evidence processing protocols.
    - Interviewing of the same person multiple times by different personnel.
    - Use of different evidence invoicing and chain of custody procedures.
    - Detention or arrest of suspects.
    - Surveillance of suspects.
    - Analysis of forensic or digital and multimedia evidence (D/MM) using different methodologies.
- Ensuring that personnel possess the subject matter expertise to conduct necessary I/I operations for an IC/UC.
- Providing an IC/UC with open-source, sensitive, and classified information and intelligence in a manner similar to how these types of information would be made available to other authorized and cleared personnel who may be responding to the incident.
- Providing a means of linking directly to federal command centers, such as the National Transportation Safety Board's Response Operations Center or the FBI's Joint Operations Center,

to provide for continual information sharing and the seamless transfer of the I/I function as needed.

- Providing coordination with other information sharing entities, including state or major urban area fusion centers, Regional Intelligence Sharing Systems (RISS) Centers, High Intensity Drug Trafficking Area Investigative Support Centers, Joint Terrorism Task Forces, and other analytic and investigative entities, as applicable.

- Providing access to information sharing tools and portals, such as the Emergency Management and Response–Information Sharing and Analysis Center (EMR–ISAC),[23] the Homeland Security Information Network (HSIN),[24] RISS,[25] Law Enforcement Online (LEO),[26] and other information sharing systems.

- Allowing an IC/UC to determine whether the incident is the result of criminal acts or terrorism, make and adjust operational decisions accordingly, and maximize efforts to prevent additional criminal activities or terrorism.

- *As permitted by local, state, tribal, territorial, insular area, and federal law:* Allowing an IC/UC to initiate I/I activities while ensuring that life safety operations remain the primary incident objective (see Figure 1). The I/I function operates concurrently with, and in support of, life safety operations to protect evidence at crime and investigative scenes.

[23] The EMR–ISAC is a component of FEMA/U.S. Fire Administration that provides critical information analysis, sanitizes classified or sensitive information, and distributes it nationally to thousands of emergency response and management entities.

[24] HSIN is a comprehensive, nationally secure, and trusted web-based platform used to facilitate sensitive but unclassified information sharing and collaboration between local, state, tribal, federal, private sector, and international partners.

[25] The RISS program is composed of six regional projects that share intelligence and coordinate efforts against criminal networks operating in many locations across jurisdictional lines. Although the six RISS projects are primarily focused on drug crime, they may select additional target crimes and provide a range of services to assist their member agencies.

[26] LEO is a controlled-access communications and information sharing data repository. It provides an internet-accessible focal point for electronic sensitive but unclassified communication and information sharing for international, local, state, tribal, and federal law enforcement agencies.

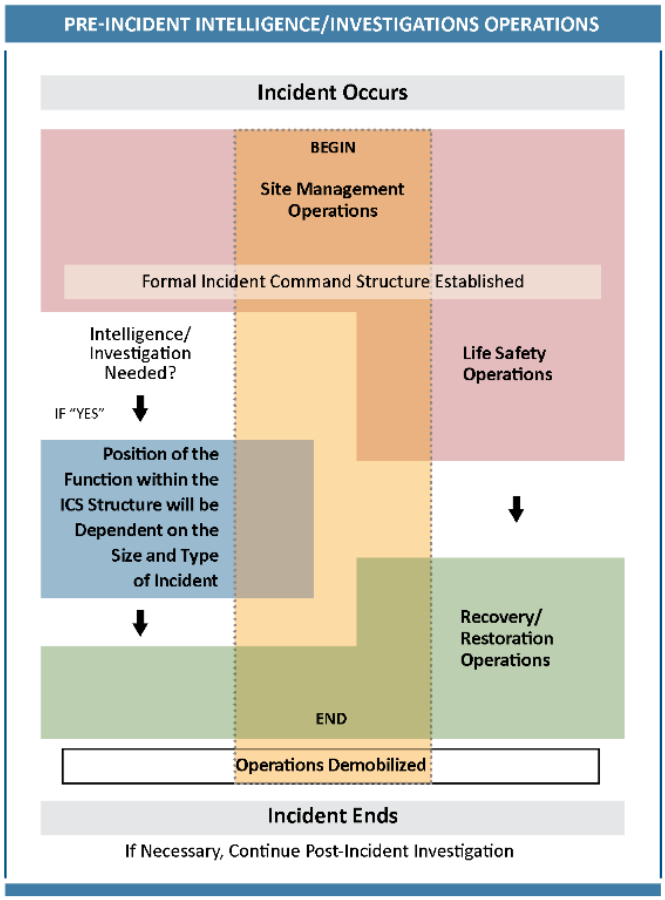

Figure 1. Example of the Flow of Events in Establishing the I/I Function

4. Incident Information

During incidents that involve I/I functional elements, I/I-related information may be required for effective incident planning, decision-making, public communications, COP, overall management of the incident, and mitigation of further effects or prevention of subsequent incidents. How that information is shared, protected, and used by appropriate stakeholders is critical to successful incident management and associated Prevention, Protection, Mitigation, Response, and Recovery functions. During an incident, personnel need timely and accurate information to make decisions. Information is used for many functions within the ICS, EOCs, MAC Groups, and JIS, including:

- Aiding in planning.
- Communicating with the public, including emergency protective measures.
- Determining incident cost.
- Determining the need for additional involvement of NGO or private sector resources.

- Identifying safety issues.
- Resolving information requests.

There is often a need to manage current intelligence gathering outside of incidents, including information gathered through the Intelligence Cycle (Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, Dissemination, Evaluation). The methodology for managing this intelligence information can cover the following:

- Transforming raw data into information for an incident.
- Feeding information from outside investigations into the incident.
- Monitoring current investigations underway outside the incident

4.1. Management of Intelligence/Investigations Incident Information

When the I/I function is incorporated into an incident and standard NIMS Communications and Information Management processes are followed, considerations for I/I information management and protection should be implemented.

Fusion Centers

Fusion centers play an important role in managing I/I-related communications and information. While normally existing outside of the NIMS command and coordination structure during the steady state, information management hubs—like fusion centers—can become an extension of the NIMS command and coordination MACS.

4.2. Incident Reports

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

- **Situation reports:** Reports typically produced and distributed on a recurring basis that contain incident details. These reports offer a snapshot of the incident status during the past operational period and contain confirmed or verified details (who, what, when, where, and how) relating to the incident. Situation reports may contain a restricted attachment or addendum with specific, sensitive I/I situation information limited to authorized decision-makers and responders with a specific need to know.
- **Status reports:** Reports, such as spot reports, that include vital and/or time-sensitive information outside regularly scheduled situation reports. Status reports are typically function-specific and less formal than situation reports.

Leaders can facilitate information processing by standardizing the information contained in situation and status reports within and across jurisdictions and organizations; however, a desire to standardize should not prevent the collection or dissemination of information unique to a reporting organization. Transmitting data in a common format enables other jurisdictions and organizations to anticipate—and rapidly find and act on—specific incident information.

4.3. Incident Action Plan

In addition to incident reports, personnel can improve situational awareness and better understand incident objectives and tactics by referring to the Incident Action Plan (IAP), which includes:

- Incident objectives that the IC or UC establishes.
- Tactics for the planned operational period, generally 12 to 24 hours.

IAPs may include restricted attachments or annexes with specific, sensitive I/I operational information limited to incident personnel with a specific need to know.

For incidents with I/I aspects, leaders may need to use a separate planning process for classified or sensitive intelligence information and tactics. This would be much like the Branch Tactical Planning Process. The Intelligence THSP working in the Planning Section should advise the IC/UC on what can be included in the unclassified IAP and who can be briefed on it. If the IAP contains classified or sensitive information and assignments, separate briefings may be required for those who have clearance or a need to know.

4.4. Information Security/Operational Security

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

4.5. Information Management Organizational Options

Within ICS, the Situation Unit in the Planning Section collects, processes, and organizes incident information. I/I personnel can be assigned to the Situation Unit to assist with the management of I/I information. This would allow I/I information to be included in the Situation Unit but managed and protected by I/I personnel. See Appendix B for more information on organizational options in the Planning Section and Situation Unit.

4.6. Data Collection and Processing

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

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

The Liaison Officer, Situation Unit Leader, and Public Information Officer (PIO) all reach out for information on the incident. They know their position role but often do not have the contacts or ability to gather specific intelligence information. By adding I/I function support to a NIMS organization, the I/I specialist can manage outside intelligence information processes and be the conduit for intelligence information. See Appendix B for more information on organizational options in the Situation Unit and Documentation Unit.

Logistics Section support is provided throughout the incident. When an incident involves I/I issues, the Communications Unit and Facilities Unit may need to provide additional, specialized support for I/I communications, IT, and facilities requirements.

4.7. Data Collection Plan

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

The record system for an incident involving I/I must include sensitive or classified storage. The Logistics Section will provide appropriate support for record systems. There also must be an appropriate information system that supports secure, sensitive, or classified intelligence information. Some systems used for IAP generation are not secure. Incident personnel must have awareness of the security of systems in use.

The EEI should be defined prior to developing a data collection plan; NIMS includes EEI examples. Information collection requirements can be set off-site, such as at a Regional Operations Center (ROC)/fusion center, or at a location specified by the Data Collection Manager (if assigned). When developing the data collection plan, the intelligence and law enforcement information and information handling may be tailored to the incident or event.

Personnel accomplish data gathering using a wide variety of methods:

- Obtaining 911 call data from public safety telecommunicators or from dispatch systems.
- Monitoring radio, video, and data communications among responders.
- Reading situation reports.
- Using technical specialists such as National Weather Service representatives.

- Receiving reports from field observers, ICPs, Area Commands, MAC Groups, DOCs, and other EOCs.
- Deploying information specialists to EOCs, other facilities, and operational field offices.
- Analyzing relevant geospatial products.
- Monitoring print, online, broadcast, and social media.

I/I raw data and information requirements may be identified and communicated through EEI, with collected information being turned over to authorized I/I personnel for validation, processing, collation, and analysis. This validation and analysis process can occur within NIMS command and coordination system elements (e.g., ICP or EOC) if I/I information management, communications, and facility requirements are met. Otherwise, this can be coordinated with steady-state I/I entities (fusion centers, agencies, or organizations using day-to-day process).

4.8. Off-site Intelligence Elements Coordination

I/I coordination may occur through existing intelligence channels, such as Joint Terrorism Task Forces, ongoing investigations, and intelligence fusion centers—including fusion centers that interface with the Incident Management Team (IMT).

4.9. Public Information

I/I personnel should work closely with PIOs and the JIS to review and validate information releases.

4.9.1. SOCIAL MEDIA

Social media activity presents unique considerations for incident management at all levels. It also provides a set of tools that can facilitate the following:

- Monitoring and gathering information and firsthand accounts of incident impacts.
- Collecting operational, investigative, and intelligence information that can assist in the identification, apprehension, and prosecution of perpetrators or prevent a future attack.
- Distributing public information and warning.
- Producing maps and incident visualizations.
- Matching available information, services, and resources to identified needs.

4.9.2. USING SOCIAL MEDIA FOR SITUATIONAL AWARENESS

Social media provides innovative ways of gathering data to achieve situational awareness. When fusion centers, law enforcement, public health, and other information entities monitor spikes or

trends in social media, they can gain enhanced situational awareness and provide early indications of emerging issues. As with all data, incident personnel use data validation processes to filter and determine the accuracy of information gained via social media.

4.10. Information Exchange and Management within NIMS Command and Coordination Systems

Successful incident management relies on the coordinated and timely exchange of information to enhance situational awareness, inform decision-making, and facilitate overall coordination and unity of effort. I/I personnel integrated with key functional elements of NIMS Command and Coordination can facilitate management and exchange of I/I-related information within the existing structures.

- I/I personnel assigned to a specific Command and Coordination element—such as an ICP or EOC—can facilitate the exchange of I/I information within that entity. For example, I/I personnel conducting fieldI/I activities in the Operations Section may exchange information with an I/I responder assigned to the Situation Unit. More specifically, an Investigation Group Supervisor (Operations Section) might coordinate with the Situation Unit (Planning Section), with the I/I responder serving as an Assistant Unit Leader or THSP focused on I/I functions.

- I/I personnel assigned to various Command and Coordination elements can facilitate the exchange of I/I information between multiple Command and Coordination entities and facilities. For example, I/I personnel assigned to an ICP may exchange information with I/I personnel assigned to an EOC.

- I/I personnel assigned to one or more Command and Coordination elements can facilitate the exchange of I/I information with steady-state I/I stakeholders external to the NIMS structure. For example, I/I personnel assigned to an ICP or EOC may exchange information with an external fusion center or I/I-associated department or agency (e.g., police department). NQS includes a qualification standard for a Fusion Liaison Officer position, which is naturally suited to perform this function.

These types of arrangements allow I/I information to be communicated and shared according to NIMS Communications and Information Management structures and processes and in alignment with existing NIMS Command and Coordination constructs. The integration of I/I personnel within NIMS Command and Coordination constructs not only facilitates information exchange but protects the integrity of the information, which is particularly important when information is sensitive or restricted.

4.11. The Intelligence Cycle: The Foundation of Intelligence Operations

Integration of the Intelligence Cycle, as defined by the Office of the Director of National Intelligence (ODNI), into the structures of NIMS and ICS bolsters strategic decision-making and situational

awareness across all phases of incident management, homeland security, and emergency response operations.[27]

The Intelligence Cycle is an essential process that transforms raw information into polished intelligence for policymakers, military commanders, and other decision-makers. This process is continuous, dynamic, and iterative, and encompasses six steps:

1. **Planning and Direction:** This initial phase involves establishing the intelligence needs of consumers and planning the subsequent intelligence activities. Direction often precedes planning, particularly when there is a specific intelligence product requirement. Depending on the need, the intelligence organization adapts its activities within the cycle to produce the desired output.
2. **Collection:** Intelligence professionals collect raw data through various sources, including Geospatial Intelligence (GEOINT), Human Intelligence (HUMINT), Measurement and Signature Intelligence (MASINT), Open-Source Intelligence (OSINT), Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT). The data can stem from multiple platforms, ranging from news reports and public documents to satellite imagery.
3. **Processing and Exploitation:** Specialized personnel and advanced technology are employed to convert raw data into a format suitable for analysis. This stage involves diverse techniques, such as data decryption, translation, and imagery interpretation, transforming the information into an analyzable asset. Staff responsible for situational awareness review data to determine if it is incomplete, inaccurate, embellished, outdated, or misleading. Personnel should use a variety of sources to validate data.
4. **Analysis and Production:** At this stage, analysts evaluate, integrate, and analyze the information to construct a comprehensive intelligence product. Situational awareness staff analyze validated data to determine its implications for incident management and to turn raw data into information that is useful for decision-making. Analysis addresses the incident's information needs by breaking those information needs into smaller, more manageable elements and then addressing those elements. Personnel should base their analysis on a thorough understanding of the problems and the situation. Personnel should provide timely and objective analysis and be cognizant of missing or unknown data. Though this phase is critical, it may be bypassed in certain scenarios when specific raw data are required, as was the case during the 1962 Cuban Missile Crisis.
5. **Dissemination:** The completed intelligence product is transmitted to the original requestor and other relevant, authorized entities only. Dissemination is often through electronic means, ensuring rapid and secure delivery of what is now termed "finished intelligence." Personnel

[27] www.DNI.gov, 2011

should disseminate incident information in a timely and accurate way, with the goal of enhancing situational awareness and encouraging effective coordination.

6. **Evaluation:** Continuous feedback is integral at all stages of the Intelligence Cycle. This ongoing evaluation refines and hones the entire process, adapting to consumers' evolving needs and ensuring that each step of the cycle is as efficient and effective as possible. Informational accuracy and completeness can help incident managers make sound decisions. Personnel can develop situational awareness by continually monitoring, verifying, integrating, and analyzing relevant elements of data and information.

The Intelligence Cycle plays a foundational role in enhancing the efficacy and coordination of NIMS and ICS, particularly in the domains of incident management and national security operations. By providing a structured sequence of processes—from planning and direction to collection, processing, analysis, and dissemination—the Intelligence Cycle serves as a versatile framework that is crucial for the systematic formulation and execution of intelligence tasks.

In the context of NIMS and ICS, this cycle is not a rigid protocol but a dynamic, iterative process that adapts to the unique demands and operational nuances of each incident or security requirement. It advocates for a proactive stance in intelligence operations, wherein continuous training, appropriate resource allocation, and regular procedural refinements help operations evolve to threats and operational needs.

Furthermore, this comprehensive integration enhances strategic coherence and operational efficiency. It ensures that intelligence functions are not ancillary but are, in fact, central to the strategic and operational decision-making process. This centrality optimizes response initiatives, informs resource deployment, and shapes tactical actions, thereby contributing to a robust, resilient, and secure operational paradigm within both NIMS and ICS frameworks.

By emphasizing adaptability, the Intelligence Cycle supports a wide array of incident management and security scenarios, demonstrating its indispensability as a cornerstone of modern intelligence operations.

5. Communications Standards and Formats

5.1. Common Terminology, Plain Language, Compatibility

The use of common terminology and plain language helps incident personnel from different disciplines, jurisdictions, organizations, and agencies communicate and coordinate activities. I/I-specific language that is not common to NIMS must be discussed, defined, and documented as appropriate for responders.

5.2. Data Interoperability

Personnel should plan, establish, and apply communications protocols to enable the dissemination of information among management, command, and support elements and cooperating jurisdictions

and organizations. For an incident with I/I-specific information, the data may have to be stored separately to maintain its sensitive or classified nature. Elements of compatible information management include:

- **Data communication protocols:** Communications procedures and protocols (including voice, data, geospatial information, internet use, and data encryption protocols) for the use or sharing of information. This element includes structuring and sharing information according to the National Information Exchange Model (NIEM).

- **Data collection protocols:** Establishing multidisciplinary and/or multijurisdictional procedures and protocols (such as use of the United States National Grid) before an incident enables standardized data collection and analysis.

- **Encryption or tactical language:** When necessary, incident management personnel and their affiliated organizations should have methodology and systems in place to encrypt information for data security. Although plain language is appropriate during most incidents, tactical language is occasionally warranted due to the nature of the incident (such as during an ongoing terrorist event). In such instances, guidance on the appropriate use of specialized encryption and tactical language should be incorporated in an incident-specific communications plan.

Conclusion

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

The I/I function within ICS provides a flexible and scalable framework that allows for the integration of I/I information and activities. The post-9/11 world requires an environment that supports the sharing of information across all levels of government, disciplines, and security domains. Situational awareness is enhanced by the I/I function through the sharing of pre- and post-incident information, intelligence, and real-time incident I/I activities. All entities involved in processing and sharing information should develop a COP—during both the steady state and an incident or planned event.

Appendix A. Intelligence/Investigations Function Field Guidance

The I/I Function Field Guidance (I/I FFG) provides guidance on command structure during incidents or planned events, regardless of type, cause, size, location, or complexity. The I/I FFG describes the I/I function as a General Staff section to illustrate the potential tasks and responsibilities within the I/I Section.

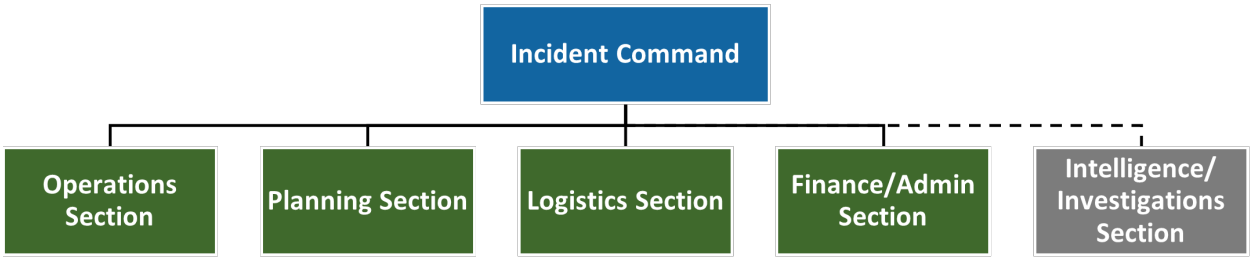

Figure 2. Intelligence/Investigations as a General Staff Section

The I/I FFG does not replace Emergency Operations Plans (EOP), laws, regulations, or ordinances. Rather, it provides guidance for personnel assigned to an incident or planned event. The information contained in the I/I FFG supplements the user's experience, training, and knowledge in the performance of I/I activities. It also provides a model for organizing and managing I/I operations and activities.

The contents of this I/I FFG are not a substitute for required formal training, I/I operations experience, and good judgment. Personnel using the I/I FFG should have a comprehensive understanding of NIMS and ICS to ensure that they can effectively set up and operate an I/I Section. All agencies and jurisdictions should ensure that responders receive adequate and appropriate training to perform their assigned I/I Section duties and tasks.

Traditional law enforcement often uses the I/I Section to investigate incidents involving possible criminal or terrorist acts. However, many other investigative entities can use the I/I function, including fire services (fire cause and origin), public health (disease outbreaks), Medical Examiner/Coroner (ME/C) (mass fatality), the National Transportation Safety Board (transportation incidents), and the Environmental Protection Agency (oil spills). No matter the incident's nature or type, personnel managing and performing I/I activities must always comply with applicable statutes,

case law, ordinances, regulations, and policies. Furthermore, the techniques they use must be authorized and lawful. Personnel managing and performing I/I activities must realize that a violation of federal, state, or local laws, regulations, or policies may have significant adverse consequences, including the suppression of critical evidence and personal civil liability.

The first part of the I/I FFG provides an overview of the I/I Section as a whole and discusses matters that apply to the General Staff level of the I/I function (such as setup, planning, logistics/communications, resource management, and coordination). The second part of the I/I FFG provides more information on groups and liaisons, coordination, and relevant task areas that can be set up under the I/I Section.

1. Intelligence/Investigations Functional Overview

The I/I FFG describes the I/I function when it is implemented as a General Staff section equivalent to other sections, such as Planning and Operations. The following section of the I/I FFG addresses considerations relevant to the I/I Section as a whole (or to the Section Chief or Deputy Section Chief). Topics covered include steps and considerations for the initial setup of the I/I Section, the use of deputies, and internal and external relationships in three areas: planning, logistics, and resource management.

1.1. Initial Setup

Following is a list of suggested tasks and actions that the IC/UC and/or the potential I/I Section Chief may consider when initially establishing the I/I Section. Users of this guide are encouraged to tailor the list, adjusting it to reflect relevant laws, policies, regulations, and incident needs.

- Collect and evaluate information while responding to the incident scene.
- Obtain a comprehensive briefing regarding the incident.
- Confer with the IC/UC regarding how the I/I Section should be established and organized.
- Assume control of the I/I Section and ensure that incident personnel are promptly notified.
- Confer with the IC/UC to determine which I/I agencies are involved in the incident, including any agencies whose involvement is required by law.
- Ensure that:
    - I/I activities are expeditiously implemented. I/I activities may be initiated concurrently with life safety operations; absent extraordinary emergency circumstances, incident objectives related to life safety operations take priority over all other incident objectives.
    - Required audio, data, image, and text communications equipment is obtained and communication procedures are implemented.

- A specific verbal or, if applicable, written I/I Section communications plan is prepared and provided to the Logistics Section.
- An Operations Section THSP is assigned to the I/I Section work area.
- An I/I Section THSP is assigned to the Operations Section work area.
- I/I Section staging areas are activated and a Staging Area Manager is designated for each staging area, as needed.
- Resources that initially responded directly to the scene and resources that are subsequently requested are:
  - Immediately identified.
  - Checked in.
  - Briefed regarding the incident, particularly the I/I aspects, and provided preliminary instructions, directions, information, data, precautions, requirements, etc.
  - Properly equipped.
  - Wearing Personal Protective Equipment (PPE).
  - Appropriately organized.
  - Tracked.
  - *If already on the scene:* Directed to continue performing the current assignments or reassigned to appropriate new assignments.
  - *If not already on the scene:* Directed to perform an initial assignment, directed to respond to a staging area, or directed to respond to an off-incident location.
- I/I-related incident objectives, strategies, and priorities are formulated and documented.

- Confer with the Operations Section, Logistics Section, and Safety Officer regarding force protection, security, health, and safety issues.
- Establish an I/I Section work area at a secure location a reasonable distance from the Operations Section work area and the ICP.
- Frequently communicate and coordinate with all crime scenes, investigative scenes, and off-incident facilities regarding the incident investigation (hospitals, local police department, state or major urban area fusion center, public health authorities, FBI Joint Operations Center, etc.).

- When necessary, assign an I/I Section THSP to the ICP.
- Designate one or more Deputy I/I Section Chiefs.
- Activate one or more groups or branches.
- Request the necessary and appropriate I/I resources and ensure a controlled response.
- Establish and activate an off-incident I/I Operations Center facility or site, where incident-related I/I operations and activities can be managed and performed to support the I/I Section.
    - Designate an I/I Operations Center Director and provide a comprehensive briefing regarding the incident, particularly the I/I aspects.

1.2. Use of Deputies

Depending on the size, scope, and needs of the incident, the I/I Section Chief has the option of appointing a Deputy I/I Section Chief (or even more than one). The Section Chief should consider the following factors when selecting a deputy.

1.2.1. QUALIFICATIONS

The Deputy I/I Section Chief should:

- Have the same qualifications and experience as the I/I Section Chief.
- Be capable of assuming the I/I Section Chief position permanently or temporarily when the Section Chief is absent.

1.2.2. RESPONSIBILITIES

The role of the Deputy I/I Section Chief is flexible; thus, a Deputy I/I Section Chief may:

- Collect and analyze incident-related information and data.
- Monitor and evaluate:
    - The current situation and estimate the potential future situation.
    - The I/I-related activities, resources, services, support, and reserves.
    - The implementation and effectiveness of the documented I/I objectives, strategies, and priorities and the I/I aspects of the IAP.
- Monitor and assess:
    - The effectiveness of the I/I Section organizational structure.

  - The performance of the I/I Section personnel and the I/I Operations Center Director and personnel.

- Identify, evaluate, and resolve I/I-related requirements and problems.
- Maintain situational awareness for the I/I Section Chief.
- Make important notifications, such as to the EOC, local intelligence unit, state or major urban area fusion center, FBI Joint Operations Center, communications dispatcher, or similar coordination points.
- Participate in Planning Section meetings, when appropriate.
- Perform specific activities and assignments as directed by the I/I Section Chief.

1.2.3. SELECTION OF DEPUTIES

Deputy I/I Section Chiefs may be members of a different agency than the I/I Section Chief. Their member agency may be one that:

- Has legal jurisdiction or geographic responsibility for the incident scene.
- Has legal jurisdiction or geographic responsibility regarding the I/I aspects of the incident.
- Has significant resources involved in the incident.
- Has been significantly affected by the incident.

1.3. Internal/External Intelligence/Investigations Activities and Relationships

Coordination is essential for effective and efficient management of any incident or planned event. When specialized resources, such as analysts or investigators, become active during an incident, the need for coordination increases, as other operational activities may conflict with I/I activities.

This section describes three aspects of how the I/I Section can perform as a whole (i.e., planning, logistics, and resource management). It addresses the internal and external activities of each aspect to define the actions within the I/I Section, as well as how they relate to other sections within the command structure. In addition to ensuring coordination, the I/I Section Chief may take several other steps to ensure adequate communication inside and outside the I/I Section. The I/I Section Chief may:

- Schedule and conduct:

- Regular meetings and briefings with the Deputy I/I Section Chiefs, Group Supervisors, Managers, and Coordinators and with the I/I Operations Center Director to review I/I status and progress.

- Periodic meetings and briefings with all I/I personnel and I/I Operations Center personnel.

- Establish and maintain liaison and integrated operations with all levels and functions of the incident management organization while adhering to the established chain of command and ICS protocols.

- *Until all relevant I/I activities have been completed:* Confer with the Command and General Staff to ensure that procedures are implemented to prevent:

  - Interference with I/I activities.

  - Disturbance of known or suspected crime scenes or investigative scenes.

  - Disturbance of decedents.

- Communicate and coordinate with the Operations Section as necessary regarding tactical I/I-related activities (such as crime scene searches, interviews at casualty collection points, processing of human remains, and epidemiological surveillance) and involve the respective legal authorities (prosecutors' office, magistrates, and courts of jurisdiction).

- Confer with the Command and General Staff to ensure that all I/I Section activity is continually coordinated.

- Confer with the Liaison Officer to ensure that I/I Section activity is coordinated with the appropriate governmental agencies, NGOs, and the private sector, including communicating through appropriate channels to the U.S. Intelligence Community, as well as the law enforcement, Homeland Security, military, and international security/liaison communities.

- Ensure that the PIO assists with public affairs and media-related activities.

- Coordinate with the PIO to ensure that public information-related activities do not violate or contravene operations security, operational security, or information security procedures.

1.3.1. PLANNING

Coordinated planning is a keystone of both NIMS and ICS. How well sections plan together can play a large role in determining the degree of success in response operations, including those related to I/I activities. In particular, staff responsible for I/I Section planning should not allow I/I-related incident objectives to conflict with overall incident strategies and objectives. In instances where a conflict may arise, sections must deconflict those issues prior to engaging in actions that could compromise the incident objectives or endanger personnel. The following tasks and responsibilities relate to the internal and external planning efforts of the I/I Section.

Internal Tasks/Responsibilities

- Analyze incident or planned event-related information and data, evaluate the current situation, and estimate the potential future situation.
- Maximize situational awareness and develop an accurate COP.
- Ensure that:
  - Required resources, reserves, services, and support are identified and requested in the appropriate manner.
  - Problems, requirements, issues, and concerns are identified and resolved.
  - I/I incident objectives and strategies are formulated and documented.
  - All of the I/I aspects and components of the IAP and the Demobilization Plan are implemented.

External Tasks/Responsibilities

- Participate in Planning Section meetings.
- Assist in reviewing incident priorities and establishing incident objectives.
- Assist in formulating and preparing the IAP and provide, as applicable, I/I Section organization chart, supporting plan, and supporting materials/attachments (maps, data, images, matrices, briefings, situation reports, and assessments).
- Confer with the Planning Section regarding:
  - Planning functions and activities.
  - The I/I aspects and components of the IAP, including incident objectives, strategies, and priorities; information on resources, reserves, services, and support; operations; and activities.
  - The I/I aspects and components of the Demobilization Plan.
  - Documentation and records management procedures, measures, and activities.
- Ensure that:
  - I/I needs are considered when incident objectives and strategies are formulated and the IAP is developed.

- Activities related to the formulation, documentation, and dissemination of the IAP and other planning activities do not violate operations security, operational security, or information security procedures, measures, or activities.

1.3.2. LOGISTICS/COMMUNICATIONS

Incidents that warrant the establishment of an I/I Section often require provisions for secure or other special communications capabilities. The following tasks and responsibilities relate to the internal and external logistics/communications efforts of the I/I Section.

Internal Tasks/Responsibilities

- Ensure that:
  - Audio, data, image, and text communications procedures, measures, and activities are implemented.
  - A verbal or written I/I Section communications plan is prepared.
  - All I/I personnel are familiar with life safety warning communications protocols used by other response organizations for imminent life-threatening situations.
- Prepare and implement an incident-specific communications plan as necessary, particularly if secure communications systems or security protocols are appropriate (including communications mechanisms used to convey critical information).
- When necessary:
  - Designate I/I Section primary and secondary system radio channels and primary and secondary point-to-point radio channels.
  - Ensure that a sufficient number of communications devices are obtained, including secure communications devices—such as secure telephone unit, secure telephone equipment, mobile Sensitive Compartmented Information Facility (SCIF), and secure video teleconference system.

External Tasks/Responsibilities

- Confer with the Logistics Section (Communications Unit Leader) regarding communications systems, guidelines, constraints, and protocols.
- Coordinate with the Logistics Section regarding the preparation of the I/I component of the communications plan.

- Ensure that audio, data, image, and text communications procedures, measures, and activities are implemented throughout the command structure to facilitate the communication of classified information, sensitive compartmented information, and sensitive information.

1.3.3. RESOURCE MANAGEMENT

I/I activities often require specialized equipment and trained personnel resources that may or may not be suited for inclusion with other incident resources. Specialized resources may require added security and confidentiality. Therefore, the I/I Section should coordinate with the Logistics Section and other Command Staff to ensure that adequate resource management processes are in place. The following tasks and responsibilities relate to the internal and external resource management efforts of the I/I Section.

Internal Tasks/Responsibilities

- Evaluate the current situation, estimate the potential future situation, determine the resource needs for one or more operational periods, and request the necessary operational and support resources (e.g., personnel, equipment, or vehicles).

- Maintain control of requested resources and ensure that requested resources do not deploy directly to the incident scene. (Follow standard ICS protocols for mobilization, dispatch, deployment, check-in, and task assignments.)

- Ensure that I/I Section staging areas are activated and a Staging Area Manager is designated for each activated staging area, as needed.

External Tasks/Responsibilities

- Confer with the Command and General Staff to identify anticipated I/I resource needs.

- Confer with the Planning Section and Logistics Section and, if necessary, the Liaison Officer regarding resource-related activities.

- Ensure that resources that initially responded directly to the scene and resources that are subsequently requested are:

    - Immediately identified.

    - Checked in (authorized for on-scene activities).

    - Briefed regarding the incident, particularly the I/I aspects, and given preliminary instructions, directions, information, data, precautions, and requirements. All such briefings must be consistent with legal requirements for the protection of information, including limiting the distribution of classified information to those with proper clearances and the need to know.

    - Equipped.

- Wearing PPE for the known or suspected threat or hazard.
- Organized according to ICS protocols.
- Tracked.
- *If already on scene:* Directed to continue performing the current assignments or reassigned to appropriate new assignments.
- *If not already on scene:* Directed to perform an initial assignment, directed to respond to a staging area, or directed to respond to an off-incident location.

1.4. Intelligence/Investigations Physical Location and Work Area

There are unique considerations for the physical location of the I/I Section in relation to the ICP and other General Staff sections. This is because of the sensitive nature of I/I operations and the need for consistent communication with the other portions of the command structure. The I/I Section work area is the location where the I/I Section Chief and appropriate staff remain. The I/I Section Chief manages, coordinates, and directs all I/I operations, functions, and activities from this work area.

Leaders selecting and maintaining the I/I Section work area location should note the importance of the following:

- Establishing the I/I Section work area at a secure location a reasonable distance from the Operations Section work area and the ICP.
- Coordinating with the Logistics Section to choose a location that:
  - Is large enough.
  - Is a reasonable and appropriate distance from the incident scene.
  - Provides safety, health, security, and force protection.
  - Provides fast and easy access and egress.
  - Provides adequate workspace.
  - Allows for expansion.
  - Permits continuous operations.
  - Provides adequate utilities, wireline and wireless communication services, sanitation, and other essential infrastructure and services.

- Conferring with the Operations Section, Logistics Section, and Safety Officer to ensure that adequate safety, health, security, and force protection measures are implemented in the I/I Section work area.
- When necessary, ensuring that:
  - The location has been searched for any force protection/security hazards, health hazards, and safety hazards.
  - Personnel are assigned to provide force protection/security regarding non-hostile unauthorized persons; persons conducting intelligence collection, surveillance, or reconnaissance activities/operations; hostile persons; emotionally disturbed persons, etc.
  - Identification, access/entry control, and badging procedures, measures, functions, and activities are implemented.

2. Groups and Structure in the Intelligence/Investigations Section

The I/I Section Chief has the option of creating one or more groups to oversee the activities of the Section. Groups that may be activated in the I/I Section are discussed below.

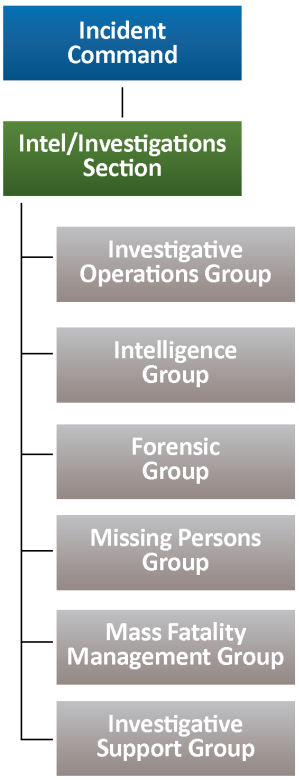

Figure 3. I/I Section Organization

2.1. Investigative Operations Group

The Investigative Operations Group is the primary group in the I/I Section. It manages and directs the overall investigative effort. The Investigative Operations Group uses the information that all the other groups and the I/I Operations Center produce to accomplish the mission of the I/I Section. The primary case investigator and primary supervisor are assigned to the Investigative Operations Group.

The Investigative Operations Group ensures that:

- An I/I plan is developed and implemented.
- Each investigative lead/task is recorded in the assignment log or database and is assigned to appropriate personnel in the proper priority order and sequence.
- Each assigned investigative lead/task is properly, completely, and expeditiously performed.
- Results of each assigned investigative lead/task are documented, and all associated materials are impounded, safeguarded, and examined.
- All forensic evidence, D/MM, and investigative evidence (e.g., documents, images, audio recordings, and data) are impounded, safeguarded, and analyzed.
- All investigative reports and materials associated with the results of each assigned investigative lead/task and the related forensic, investigative, and D/MM are discussed with authorized personnel; reports, materials, and evidence should also be examined and evaluated to determine whether the assigned investigative lead/task was properly performed.
- Each examined and evaluated investigative lead/task is categorized as closed (no further action or new leads generated) or open (additional action required).
- Information regarding each closed investigative lead/task is recorded in the assignment log or database.
- Results of each assigned investigative lead/task are exploited and, if applicable, additional follow-up investigative leads/tasks are identified, recorded, assigned, performed, etc.
- A chronological record of the significant I/I information, activities, decisions, directives, and results is maintained and, if appropriate, displayed on situation boards or a web log.
- I/I techniques and tactics are used in the proper priority order.
- Required legal advice, services, documents, applications, and processes are obtained.
- Documentation and records management procedures are implemented and followed.

- The Intelligence Group examines and analyzes all unassigned, assigned, and completed investigative leads/tasks.
- The I/I Operations Center and all of the groups communicate and coordinate with the Investigative Operations Group.
- A designated investigative supervisor or investigator is assigned to each of the crime scenes and each of the significantly involved investigative scenes, hospitals, and off-incident facilities.
- The Investigative Operations Group uses techniques and tactics including but not limited to:
    - Nontechnical and technical canvasses.
    - Interviews and interrogations.
    - Prisoner debriefings.
    - Identification procedures.
    - Searches and seizures.
    - Database/record queries.
    - Electronic communication (e.g., telephone, computer) investigative records acquisition and analysis.
    - Physical surveillance.
    - Electronic surveillance.
    - Acquisition and analysis of records and other evidence.
    - Polygraph examinations.
    - Electronic surveillance including monitoring probative social media, internet, and other cyber sources of information.
    - Activation and use of tip lines, hotlines, and call centers.
    - Human Intelligence operations.
    - Obtaining and securing of sources of investigatory data, such as flight data recorders, cockpit voice recorders, vehicle electronic data recorders, radar data, and 911 tapes.

Depending upon the scope, complexity, and size of the I/I Section, the Investigative Operations Group Supervisor may activate one or more of the positions below. As the configuration of the ICS

organization is flexible, the IC/UC may choose to combine these positions or create teams to perform the following functions:

- Assignment Manager.
- Recorder.
- Evidence Manager.
- Physical Surveillance Coordinator.
- Electronic Surveillance Coordinator.
- Electronic Communication Records Coordinator.
- Interview/Interrogation Coordinator.

2.2. Intelligence Group

The Intelligence Group is responsible for three major functions: (1) information/intelligence management; (2) operations security, operational security, and information security; and (3) information intake and assessment (when necessary).

Information/intelligence management activities include but are not limited to:

- Ensuring that:
  - Tactical and strategic I/I information is collected using appropriate, authorized, and lawful techniques and activities.
  - Intelligence requirements are used to manage and direct intelligence collection efforts.
  - Database and record queries are performed.
  - Language translation and deciphering and decryption services are provided.
  - Social media and other internet sources of information are examined and monitored.
  - I/I information is documented, secured, organized, evaluated, collated, processed, exploited, and analyzed.
  - Intelligence information needs, requests for intelligence, intelligence gaps, and standing and ad hoc intelligence requirements are identified, documented, analyzed, validated, produced (if applicable), and resolved.
  - Requests for I/I information are made to the appropriate governmental agencies, NGOs, private sector entities/individuals, the media, and the public.

  - Finished and, if appropriate, raw I/I information is documented and produced as needed (records, data, warnings, situation reports, briefings, bulletins, assessments, etc.).
  - Unclassified or lesser classified tearline reports are produced regarding appropriate classified information.
  - Classified information, access-controlled sensitive compartmented information, and/or caveated/restricted information is sanitized for use in creating and investigating leads/tasks, publishing intelligence products, and preparing warrant applications and accusatory instruments.
  - I/I information, documents, requirements, and products are appropriately disseminated.
  - Threat information/intelligence is immediately transmitted to the IC/UC, the Operations Section Chief, and, if necessary, other authorized personnel.
- Notifying and conferring with subject matter experts.
- Identifying and collecting I/I information.
- When applicable, ensuring that requests for I/I information are documented, analyzed, managed, and resolved.
- Conferring with the Planning Section regarding information/intelligence-related activities, as needed.

Operations security, operational security, and information security activities include but are not limited to:

- Ensuring that:
  - Operations security, operational security, and information security procedures and activities are implemented.
  - Classified information is disseminated to personnel who have the required clearance, access, and need to know, and is disseminated in compliance with all associated caveats.
  - Sensitive information is disseminated to authorized personnel who have the required need to know, in strict compliance with applicable restrictions and laws.
- Maintaining liaison through appropriate channels with the Intelligence Community, intelligence components of other agencies affected by the incident, and fusion centers.
- Conferring with the Command and General Staff to ensure that the confidentiality and security of I/I activities are not compromised.

Information intake and assessment activities ensure that all incoming information, with the exception of results of investigative leads/tasks, is:

- Communicated directly to the Intelligence Group.
- Documented on an information control form or entered into an information control database.
- Evaluated to determine the correct information security designation (e.g., classified or sensitive) and the required information security procedures.
- Initially evaluated and categorized as information that:
    - May require the Investigative Operations Group to assign an investigative lead/task (this information is communicated to the Investigative Operations Group for final determination regarding whether an investigative lead/task is assigned).
    - Constitutes intelligence but does not require the Investigative Operations Group to assign an investigative lead/task (absent unusual circumstances, this information is communicated to the Investigative Operations Group).
- Assessed via appropriate databases or records queries.
- Analyzed to determine whether the incoming information is related to any existing information.
- Disseminated to the appropriate I/I Section and I/I Operations Center personnel.

Depending upon the size, complexity, and scope of the I/I Section, the Intelligence Group Supervisor may activate one or more of the following positions:

- Information Intake and Assessment Manager.
- Requirements Coordinator.
- Collection Coordinator.
- Processing and Exploitation Coordinator.
- Analysis and Production Coordinator.
- Dissemination Coordinator.
- Critical Infrastructure and Key Resources Protection Coordinator.
- Classified National Security Information Security Officer.
- Requests for Information Coordinator.

As the configuration of the ICS organization is flexible, the IC/UC may choose to combine these functions or create teams to perform these functions.

2.3. Forensic Group

The Forensic Group is responsible for managing crime scenes and directing the processing of forensic evidence, D/MM, and decedents. The Forensic Group also ensures that the proper types of examinations, analyses, comparisons, and enhancements are performed on the forensic evidence, D/MM, and decedents in the proper sequence by the appropriate laboratories, analytical service providers, and morgues. The Forensic Group coordinates with the Mass Fatality Management Group and the ME/C on matters related to the examination, recovery, and movement of decedents.

The Forensic Group is responsible for ensuring that:

- The number of crime scenes and decedents, and the location of each crime scene and decedent, are expeditiously and properly determined.
- The size, configuration, boundaries, and related characteristics of each crime scene are properly determined, with each crime scene being sufficiently large.
- Each crime scene and decedent is secured and safeguarded, and access to each crime scene and decedent is controlled, restricted, and limited.
- The contamination, alteration, loss, destruction, etc., of forensic evidence, D/MM, and decedents are prevented.
- The rank/title, name, command/unit, agency, employee identification number, etc. are documented for each person who enters a crime scene or touches, searches, disturbs, or moves decedents.
- Personnel who process crime scenes and decedents confer with the primary case investigator, the primary case supervisor, the ME/C, and other appropriate personnel.
- Each crime scene and decedent is expeditiously processed in an appropriate manner and in the proper priority order and sequence.
- Forensic evidence, D/MM, and decedents are expeditiously and appropriately delivered to one or more suitable laboratories, analytical service providers, and/or morgue facilities.
- The receiving laboratory, analytical service provider, and/or morgue examines, analyzes, and compares forensic evidence, D/MM, and decedents in priority order. The Forensic Group also ensures that the proper number and types of examinations, analyses, comparisons, etc. are performed in the proper sequence.

- Personnel who process crime scenes and decedents, the primary case investigator, and the primary case supervisor confer with the appropriate laboratory, analytical service provider, and morgue personnel.
- Forensic evidence, D/MM, and decedents are delivered to a designated facility or site at an appropriate time for storage and are secured, retained, and disposed of in a proper manner at an appropriate time.
- Forensic debris and post-blast crime scene activities are implemented (when necessary).
- Crime scene reconstruction techniques and subject matter experts are used, as needed.
- Records and reports are prepared regarding forensic evidence, D/MM, and decedents.
- Crime scenes, including decedents located at crime scenes, are not prematurely released.

Depending upon the size, complexity, and scope of the I/I Section, the Forensic Group Supervisor may activate one or more of the following positions:

- Crime Scene Coordinator.
- Post-Blast Evidence Coordinator.
- Chemical, Biological, Radiological, Nuclear/Hazardous Materials Evidence Coordinator.
- Forensic Evidence Analysis Manager (including D/MM).

2.4. Missing Persons Group

The Missing Persons Group directs missing persons operations and activities, as well as Family Assistance Center activities involving missing persons. The Missing Persons Group is responsible for ensuring that:

- Missing persons information reporting is unified and centralized as much as is feasible, including the implementation of documentation, security, assessment, categorization, consolidation, tracking, storage, and dissemination activities.
- Authorized information and instructions regarding the proper procedures for reporting missing persons information are disseminated—in communication and coordination with the PIO—to the media, the public, governmental agencies, NGOs, and private entities or individuals.
- Each reported missing person is accounted for using objective criteria, that the related required notifications are made in a timely manner to the appropriate persons, and that the required information is appropriately and centrally documented. Required information includes the number of reported:

  - Potential missing persons.
  - Actual missing persons.
  - Actual missing persons located.
- Required information regarding missing persons (data, records, images, DNA reference samples, investigative evidence, forensic evidence, D/MM, and non-evidence property) is obtained at Family Assistance Centers or appropriate facilities/areas.

Depending upon the size, complexity, and scope of the I/I Section, the Missing Persons Group Supervisor may activate one or more Missing Persons Coordinator(s) or Family Assistance Center Coordinator(s).

Because the configuration of the ICS organization is flexible, the IC/UC may choose to combine these functions or create teams to perform these functions.

The Missing Persons Group Supervisor is responsible for ensuring that coordination and information documentation are established with the Forensic Group, the Mass Fatality Management Group, and the ME/C, when activated.

2.5. Mass Fatality Management Group

The Mass Fatality Management Group directs I/I activities involving mass fatality operations. These include I/I-related Family Assistance Center activities involving decedents and unidentified persons.

The Mass Fatality Management Group is responsible for ensuring that:

- Mass fatality management operations and activities are implemented.
- Decedent information reporting, documentation, security, assessment, categorization, consolidation, tracking, storage, and dissemination activities are implemented.
- Disaster Mortuary Operational Response Teams or other similar resources are requested, when necessary.
- Debris sifting operations are implemented, when necessary.
- All decedents are identified, related required notifications are made in an appropriate and timely manner to the appropriate persons, and the required information is documented in an appropriate manner.
- Mass fatality-related public health hazards are mitigated.
- The ME/C expeditiously determines the cause and manner of death of each decedent and determines the final disposition of each decedent's remains.

- Families are regularly briefed on the progress of the medicolegal operation including the recovery, examination, identification, death certification, and disposition of remains.
- The appropriate authority expeditiously issues a death certificate for each decedent.
- Required information, data, records, images, DNA reference samples, investigative evidence, forensic evidence, D/MM, and non-evidence property regarding decedents are obtained at Family Assistance Centers or appropriate facilities/areas.

Depending upon the size, complexity, and scope of the I/I Section, the Mass Fatality Management Group Supervisor may activate the following positions:

- Mass Fatality Management Coordinator.
- Field Site/Recovery Coordinator.
- Morgue/Postmortem Examinations Coordinator.
- Victim Identification Coordinator.
- Family Assistance Center Coordinator.
- Quality Assurance Coordinator.

As the configuration of the ICS organization is flexible, the IC/UC may choose to combine these functions or create teams to perform these functions.

The Mass Fatality Management Group Supervisor is responsible for ensuring that coordination and information sharing are established between the Missing Persons Group and the Forensic Group.

2.6. Investigative Support Group

The I/I Section may require the use of specialized operational and support resources. The Investigative Support Group works closely with the Command and General Staff, particularly the Logistics Section and Planning Section, to ensure that necessary resources, services, and support are obtained for the I/I Section.

The Investigative Support Group is responsible for ensuring that:

- I/I Section staging areas are activated, with each staging area situated at an appropriate location and a Staging Area Manager designated for each.
- Personnel, equipment, vehicles, aircraft, watercraft, supplies, facilities, infrastructure, networks, and other operational and support resources are expeditiously ordered and obtained.
- Food and beverages are provided to personnel as needed.

- Technical and nontechnical services and support are expeditiously ordered and obtained.
- Resources, services, and support that must be procured are identified, ordered, and obtained in a timely manner.
- Resources are maintained, repaired, replaced when necessary, safeguarded, tracked, documented, used, and retrieved.
- Accountability procedures and activities are implemented for operational and support resources.
- Resources are recovered and/or demobilized when no longer needed.
- Records and reports are prepared regarding investigative support activities.

Depending upon the size, complexity, and scope of the I/I Section, the Investigative Support Group Supervisor may activate one or more of the following positions:

- Staging Area Managers, who have the following responsibilities:
    - Properly documenting information about responding resources.
    - Categorizing and separating responding personnel based upon one or more of the following criteria:
        - Agency jurisdiction and legal authority.
        - Personnel technical skills.
        - Personnel nontechnical skills.
        - Personnel clearance and access.
        - Personnel proficiency.
    - Ensuring that:
        - Personnel resources are properly credentialed.
        - Identification, access/entry control, and badging procedures and measures are implemented.
        - Personnel resources are equipped and wearing required PPE.
        - Personnel resources are organized.

  - Personnel resources receive a briefing regarding the incident, particularly the I/I aspects, and are provided preliminary instructions, directions, information, data, precautions, and requirements.
  - Personnel resources are deployed and assigned or are directed to remain as reserves.
  - Resources are tracked.

- I/I Section Work Area Manager, who has the following responsibilities:
  - Ensuring that the I/I Section work area is maintained in an orderly manner.
  - *In coordination with the Logistics Section:* Ensuring that all of the utilities, wireline and wireless communication services, sanitation, accommodations, infrastructure, and other essential services and support-related requirements are satisfied.
- Resource Coordinator, who has the following responsibilities:
  - *If a significant number of I/I resources are required:* Working directly with counterparts in the Logistics Section to order resources and in the Planning Section to account for all resources.
  - Ensuring that:
    - Technical and nontechnical services and support are expeditiously ordered and obtained.
    - Resources, services, and support that must be procured are identified, ordered, and obtained in a timely manner.
    - Resources are maintained, repaired, replaced when necessary, safeguarded, tracked, documented, used, and retrieved.
    - Accountability procedures and activities are implemented regarding operational and support resources.
    - Resources are recovered and/or demobilized when no longer needed.
- Communications Coordinator, who works directly with the Logistics Section and has the following responsibilities:
  - Ensuring that:
    - Audio, data, image, and text communications procedures and activities are implemented.
    - A sufficient number of communication devices, including secure communication devices, are obtained, maintained, repaired, replaced when necessary, safeguarded, appropriately distributed, tracked, documented, used, and retrieved.

  - Radio channels are monitored at the I/I Section work area.
  - The I/I Section communications plan is prepared and updated and is communicated to the Logistics Section.
- Ascertaining the designated *system* radio channels and *point-to-point* radio channels that are being used for the incident.
- Designating the I/I Section system radio channels and point-to-point radio channels, as needed.

- Physical Security Coordinator, who has the following responsibilities:
  - Ensuring that adequate physical security measures are in place. (This position does not have authority to implement site security actions.)
  - Conferring with the Operations Section, Logistics Section, and Safety Officer regarding personnel safety plans, procedures, and activities.
  - Ensuring that:
    - All involved areas are searched for force protection and security, health, safety, and environmental hazards.
    - All force protection and security, health, safety, and environmental hazards are identified, addressed, and resolved.
    - All dangerous or hazardous people, weapons, devices, objects, animals, and conditions are identified, isolated, controlled, and safely mitigated.
    - Actual and potential threats are identified, investigated, and resolved.
    - Identification, access/entry control, and badging procedures and measures are implemented.
    - Personnel safety procedures and measures are implemented regarding the I/I Section work area.

As the configuration of the ICS organization is flexible, the IC/UC may choose to combine these functions or create teams to perform these functions.

Appendix B. Incident Command System

NIMS states that the purpose of the I/I function within ICS is to do the following:

- Prevent and deter potential unlawful activity.
- Collect, analyze and disseminate information, intelligence, and situational awareness.
- Identify, document, collect, safeguard, and analyze evidence and specimens.
- Conduct thorough and comprehensive investigations that lead to a perpetrator's identification, apprehension, and successful prosecution.
- Inform and support life safety operations.
- Determine the source or cause of an 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.

These functions are typically performed by staff in the Operations and Planning Sections. However, for incidents that involve or may involve a significant level I/I work, the IC or UC may choose to consolidate the I/I function in the ICS organization in a number of ways. The I/I function's location in the ICS structure depends on factors such as the nature of the incident, the level of I/I activity involved or anticipated, and the relationship of the I/I activities to the other incident activities. The I/I function can be incorporated as an element of the Planning Section, in the Operations Section, within the Command Staff, as a separate General Staff section, or in some combination of these locations. Figure 4 depicts the various locations where the IC or UC might opt to locate the I/I function.[28]

The Liaison Officer, Situation Unit Leader, and Public Information Officer all reach out for information on an incident. They know their position role but often do not have the contacts, skill, or ability to gather specific intelligence information. By adding an Intelligence Specialist or Assistant Liaison Officer for Intelligence, leaders can provide a conduit for intelligence information and ensure that outside intelligence information processes are managed. Much as a Safety Officer might assign an Assistant Safety Officer with skills and abilities for a specific hazard area, a Liaison Officer might assign an Assistant Liaison Officer for Intelligence with the appropriate intelligence skills and abilities to coordinate with external intelligence sources, like a ROC/fusion center. Intelligence would be scrubbed for sensitivity, then fed into the incident. If incident personnel do not reach out to these

[28] FEMA, National Incident Management System, October 2017.

outside areas, a vacuum of intelligence information arises that can adversely affect the incident response. Adding a position would not require creating a separate organization in the incident but could provide support for the Liaison Officer or the Situation Unit Leader.

As the configuration of the ICS organization is flexible, the IC/UC may choose to combine I/I functions or use multiple I/I organizational options. The nature and specifics of an incident, in addition to legal constraints, could restrict the type and scope of information that may be readily shared. When that information affects or threatens the life safety of the responders or the public, the information can and should be shared with appropriate Command and General Staff. The IC/UC should consider the different options and, using NIMS principles, start at the lowest level and build up as appropriate.

Life safety is always the primary incident objective. The establishment of the I/I function in these various options does not diminish or alter this primary objective. It enhances the primacy of the life safety incident objective. For example, evidence recovered from the incident scene and the information produced from I/I activities may prevent a subsequent criminal or terrorist act from occurring at the incident site or other locations.

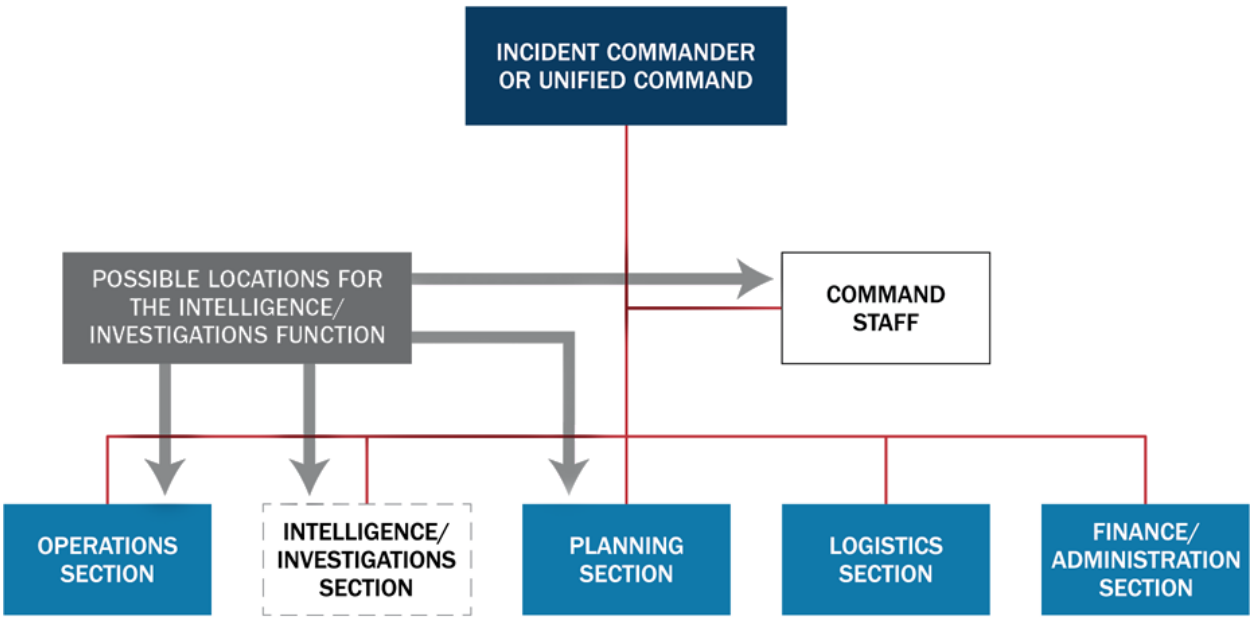

Figure 4. Options for the Placement of the I/I Function

1. Intelligence/Investigations Functions in the Incident Command System

1.1. Intelligence/Investigations Function in the Planning Section

Integrating the I/I function in the Planning Section—either as part of the Situation Unit or as a separate I/I Unit—enhances the section's normal information collection and analysis capabilities. It helps ensure that Planning Section staff benefit from streamlined information sharing; investigative information, resources, and tools; and the I/I personnel's analytic and subject matter expertise.[29]

Though the Situation Unit Leader typically manages internal intelligence information, the leader may bring in a THSP to take on this role. An Intelligence THSP may manage I/I debriefs and develop scrubbed output for the incident. If the IAP has separate sensitive or classified portions, the Intelligence THSP may provide the operational period briefing on these portions.

In addition, if a Data Collection Manager is assigned to the Situation Unit, appropriate training and expertise will be required to ensure appropriate information management cycle processing (including appropriately cataloging information, turning it into appropriate products, and ensuring those who need the sensitive I/I information get it).

If the information management requirements exceed the Situation Unit's ability to effectively manage I/I information—even with I/I staff augmentation—the inherent flexibility and scalability of the ICS organization allows for alternative organizational options. One possibility is the establishment of an additional unit in the Planning Section (I/I Information Unit) to manage I/I information. The responsibilities of this unit would likely mirror those of the Situation Unit, with a specific focus on I/I information. To ensure overall situational awareness and a COP, this I/I-specific unit and the Situation Unit would need to collaborate closely on information management.

1.2. Intelligence/Investigations Function in the Operations Section

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

[29] FEMA, National Incident Management System, October 2017.

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

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

1.3. Intelligence/Investigations Function in the Command Staff

When an incident has an I/I dimension but does not currently have active I/I operations, the IC or UC may assign I/I personnel to serve as command advisers, as I/I Officers, or as Assistant Liaison Officers. Command advisers would be I/I THSPs who interface with their parent organizations and provide subject matter expertise to incident leaders. Subject matter expertise can also come through an assigned I/I Officer or Assistant Liaison Officer. Integrating the I/I function into the Command Staff helps ensure that I/I personnel have immediate and constant access to the IC, UC, and other members of the Command Staff, such as legal advisers, the Safety Officer, and the PIO. This in turn helps ensure that incident leaders understand the implications and potential second-order effects of incident management decisions and activities from an I/I standpoint.[30]

As noted above, one option is assigning an Assistant Liaison Officer for I/I. This position would coordinate with off-site I/I entities much like an Assistant Liaison Officer assigned to coordinate with the ROC, fusion centers, and EOCs for information.

1.4. Intelligence/Investigations Function as a Standalone General Staff Section

The IC or UC may establish the I/I function as a General Staff section when there is a need to manage the I/I aspects of the incident separately from the other incident management operations and planning. This may occur when the incident involves an actual or potential criminal or terrorist act or when significant investigative resources are involved, such as for an epidemiological investigation that requires use of a separate section.

1.5. Use and Organization of Groups

Under NIMS, sections may be organized into branches, groups, and divisions to meet the needs, scale, and complexity of an incident or event. If necessary to manage span of control, divisions may be established as needed.

[30] FEMA, National Incident Management System, October 2017.

Due to the functional nature of I/I activities, groups may be established representing specific mission areas. These groups may be created within the Operations Section or within a separate I/I Section. The Section Chief may create one or more groups within the section and designate a Group Supervisor for each group. The Section Chief is expected to notify the Planning Section and IC, when applicable, regarding the number of personnel assigned to the section and to each group. If any of the groups are not used or have been deactivated, the Section Chief manages those responsibilities.

As permitted by local, state, tribal, territorial, insular area, and federal law, groups are used based on the needs of the incident. Groups that may be activated in the Operations Section or I/I Section include:

- **Investigative Operations Group:** Responsible for overall investigative effort.
- **Intelligence Group:** Responsible for obtaining, analyzing, and managing unclassified, classified, and open-source intelligence.
- **Forensic Group:** Responsible for collection and integrity of physical evidence and the integrity of the crime scene.
- **Missing Persons Group:** Responsible for directing the missing persons investigations and activities, as well as Family Assistance Center activities involving missing persons.
- **Mass Fatality Management Group:** Responsible for directing the I/I activities involving mass fatality management operations.
- **Investigative Support Group:** Responsible for ensuring that required investigative personnel are made available expeditiously and that the necessary resources are properly distributed, maintained, safeguarded, stored, and returned, when appropriate.

1.6. Use and Organization of Branches

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

1.6.1. GEOGRAPHIC BRANCHES

The Section Chief establishes geographic branches to maintain a manageable span of control in the section by grouping two or more divisions and/or groups. The boundaries of geographic branches are thus defined by the combined areas of the divisions that make up each branch.

1.6.2. FUNCTIONAL BRANCHES

The Section Chief establishes functional branches to maintain a manageable span of control in the section by grouping two or more divisions and/or groups that have similar functions. For example, if a large aircraft crashes in a local jurisdiction, various disciplines (including law enforcement, fire,

EMS, public works, and public health) may each have a functional branch operating under a single Operations Section Chief's direction. The Section Chief may organize around different functional groups, depending on the jurisdiction's plan and the incident type.

1.7. Preparedness

Prior to the start of a planned event (such as a parade, concert, convention, sporting event, or National Special Security Event), the I/I function can be used to foster information sharing and collaboration. It can also provide the information and intelligence necessary to ensure that planning activities are fully informed.

Furthermore, as the result of a credible threat of criminal or terrorist activity, an I/I organization may be activated and operations may be initiated prior to a potential incident. If an incident subsequently occurs, the I/I function should incorporate the appropriate elements of the pre-incident I/I organization and use the pre-incident information and intelligence that was collected.

It is vital to plan for the possibility that an incident may escalate beyond the resources of a local community. Therefore, preparedness activities should include planning for the response of federal resources and personnel. Activities should also include the transfer of primary investigative and prosecutive jurisdiction and responsibility from local to federal agencies in keeping with applicable laws, regulations, and policies.

Appendix C. List of Abbreviations

AHJ	Authority Having Jurisdiction
COP	Common Operating Picture
CPG	Comprehensive Preparedness Guidance
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DOC	Department Operations Center
D/MM	digital and multimedia evidence
EEI	essential elements of information
EMR–ISAC	Emergency Management and Response–Information Sharing and Analysis Center
EMS	Emergency Medical Services
EOC	emergency operations center
EOP	Emergency Operations Plan
FBI	Federal Bureau of Investigation
FIOP	Federal Interagency Operational Plan
FIRESCOPE	Firefighting Resources of California Organized for Potential Emergencies
GEOINT	Geospatial Intelligence
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
I/I	Intelligence/Investigations
I/I FFG	Intelligence/Investigations Function Field Guidance
IAP	Incident Action Plan

IC	Incident Commander
ICP	Incident Command Post
ICS	Incident Command System
IMT	Incident Management Team
JIC	Joint Information Center
JIS	Joint Information System
LEO	Law Enforcement Online
MAC Group	Multiagency Coordination Group
MACS	Multiagency Coordination System
MASINT	Measurement and Signature Intelligence
MOU	Memorandum of Understanding
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NGO	Nongovernmental Organization
NPG	National Preparedness Goal
NQS	National Qualification System
NRCC	National Response Coordination Center
ODNI	Office of the Director of National Intelligence
OSINT	Open-Source Intelligence
PII	Personally Identifiable Information
PIO	Public Information Officer
PKEMRA	Post-Katrina Emergency Management Reform Act
PPD	Presidential Policy Directive
PPE	Personal Protective Equipment

PTB	Position Task Book
RIS	Resource Inventory System
RISS	Regional Intelligence Sharing Systems
ROC	Regional Operations Center
RTLT	Resource Typing Library Tool
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SIGINT	Signals Intelligence
THSP	Technical Specialist
UC	Unified Command

Appendix D. Glossary of Terms

analysis: The comprehensive and systematic examination, assessment, and evaluation of collected, processed, and exploited information/intelligence to identify significant facts, ascertain trends and patterns, develop alternative options, forecast future events, and derive valid conclusions.

branch: The organizational level having functional or geographical responsibility for major aspects of incident operations. 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.

caveat: A prohibition regarding the dissemination, sharing, distribution, or delivery of information/intelligence. Dissemination caveats are not a level of classification but are used in conjunction with the appropriate classification level. The following are examples of dissemination caveats:

- ORCON (Dissemination and Extraction of Information Controlled by Originator): No further dissemination can occur without the prior approval of the originating entity that provided the subject information/intelligence.
- NOFORN (Not Releasable to Foreign Nationals): May not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens.
- REL TO: Authorized for release to (specify one or more countries).
- RELIDO: Releasable by Information Disclosure Officer.

classified national security information (also referred to as *classified information*): Any data, file, paper, record, or computer screen containing information associated with the national defense or foreign relations of the United States and bearing the markings Confidential, Secret, or Top Secret. This information has been determined, pursuant to Executive Order 13526 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status. There are three levels of classified information:

- Confidential: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
- Secret: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

- Top Secret: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

collection: The gathering of information through approved techniques to address and/or resolve intelligence requirements. The sources of information that are used during the Collection step of the Intelligence Cycle include Human Intelligence, Signals Intelligence, Geospatial Intelligence, Imagery Intelligence, Open-Source Intelligence, and Measurement and Signature Intelligence.

Command Staff: The staff that reports directly to the Incident Commander, including the Public Information Officer, Safety Officer, Liaison Officer, and other positions. Command Staff may have an assistant or assistants, as needed.

controlled unclassified information (CUI): Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526[31] or the Atomic Energy Act, as amended.[32]

coroner: The official, in coroner jurisdictions, charged with the medicolegal investigation of deaths and fatality management. This individual is responsible for certifying the identification and determining the cause and manner of death of deceased persons, or decedents. The coroner has statutory jurisdiction over all bodies and decedents falling within the geographic jurisdiction and within certain prescribed categories of death. Mass fatality incidents may involve victims who are within those statutorily prescribed categories.

crime scene: An area or areas containing physical evidence or decedents that may have forensic, investigative, digital/multimedia, demonstrative, or other probative value. Crime scenes include casualty collection areas and fatality collection points.

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.

decedent: Any human body or portion thereof that is clinically deceased. Decedents include whole bodies, body parts, and body fragments, including unassociated tissue.

deconfliction: The avoidance of duplication or interference.

[31] https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002 | 32 CFR

[32] https://www.archives.gov/files/isoo/policy-documents/eo-13556.pdf | E.O 13556

digital evidence: Physical evidence consisting of information of probative value that is stored or transmitted in binary form.

digital and multimedia evidence (D/MM): Electronic physical evidence that does or may require scientific examination, analysis, comparison, and/or enhancement. D/MM includes electronic text, data, audio, and image evidence, such as video, closed-circuit television, photograph, camera, computer, radio, personal information management device, wireline telephone, wireless telephone, smartphone, satellite telephone, Wi-Fi messaging device, digital multimedia device, pager, navigational system/GPS, storage device/media, server, network device, wireless device, modem, antenna, peripheral device, telephone caller identification device, audio recording device, answering machine, and facsimile machine.

Director of National Intelligence: Position created pursuant to the Intelligence Reform Act of 2004. The Director of National Intelligence has "executive authority" to oversee the U.S. Intelligence Community.

emergency operations center (EOC): A facility from which staff provide information management, resource allocation and tracking, and advanced planning support to personnel on scene or at other EOCs (e.g., a state center supporting a local center).

force protection and security: Protecting responders from hazards involving one or more persons, weapons, devices, objects, animals, conditions, or situations.

forensic evidence: Nonelectronic physical evidence that requires (or may require) scientific examination, analysis, comparison, and/or enhancement.

forensics: The use of science and technology to investigate and establish facts in criminal or civil courts of law.

fusion: The overarching process of managing the flow of information and intelligence across all levels and sectors of government and the private sector.

General Staff: A group of incident management personnel organized according to function and reporting to the Incident Commander (IC). The General Staff normally consists of the Operations Section Chief, Planning Section Chief, Logistics Section Chief, and Finance/Administration Section Chief. An I/I Section Chief may be designated, if required, to meet incident management needs.

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 division.

Human Intelligence: Intelligence information acquired by human sources through covert and overt collection techniques.

Imagery Intelligence: The collection, analysis, and interpretation of conventional, analog, and digital image information/data.

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

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

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

incident objectives: Statements of guidance and direction needed to select appropriate strategies and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been effectively deployed. Incident objectives should be achievable and measurable, yet flexible enough to allow strategic and tactical alternatives.

information management (in NIMS): Collection, organization, and control over the structure, processing, and delivery of information from one or more sources, and subsequent distribution to one or more audiences who have a stake in that information.

information security/operational security (in NIMS): The policies, practices, and procedures that ensure that the information/intelligence stored, processed, transmitted, etc., using IT systems and networks is secure and not vulnerable to inappropriate or unauthorized discovery, access, export, use, modification, etc. The need for confidentiality sometimes complicates sharing information. This can be particularly pronounced when sharing intelligence within the law enforcement community and with the emergency management, fire, public health, and other communities. Access to certain restricted or classified information depends on applicable law, as well as an individual's security clearance and need to know.

insular area: A U.S. associated jurisdiction that is not part of a U.S. state or the District of Columbia.

intelligence: Generally speaking, information that has been evaluated and from which conclusions have been drawn to make informed decisions. Intelligence can be defined slightly differently depending on the agency or organization of focus. Types of intelligence include:

- Raw intelligence: Unevaluated collected information/intelligence, usually from a single source, that has not been fully processed, exploited, integrated, evaluated, analyzed, and interpreted.
- Finished intelligence: The product, usually from multiple sources, resulting from the processing, exploitation, integration, evaluation, analysis, and interpretation of collected

information/intelligence that fully addresses an issue or threat based upon available information/intelligence.

- Strategic intelligence: Information tailored to support the planning and execution of agencywide intelligence and investigative programs, and the development of long-term policies, plans, and strategies.
- Tactical intelligence: Information that directly supports ongoing operations and investigations.

intelligence (in NIMS): Threat-related information developed by law enforcement, medical surveillance, and other investigative organizations.

Intelligence and Information Sharing (PPD-8, NPG, core capability): Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

Intelligence Cycle: An essential process that transforms raw information into polished intelligence for policymakers, military commanders, and other decision-makers. This process is continuous, dynamic, and iterative, encompassing six steps: Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, Dissemination, Evaluation.

intelligence gap: An unanswered question regarding a criminal, cyber, or national security issue or threat.

intelligence information need: The information/intelligence needed to eliminate one or more intelligence gaps and/or to support the mission of the governmental agency, Nongovernmental Organization (NGO), or private entity/individual submitting the intelligence information need.

Intelligence Information Report: The standard product used to document raw information/intelligence and to disseminate the raw information/intelligence to national policymakers, the U.S. Intelligence Community, the Homeland Security community, and the law enforcement community. Analysts use Intelligence Information Reports and other available sources of information/intelligence to produce finished information/intelligence.

Intelligence/Investigations function: Efforts to determine the source or cause of an incident (e.g., disease outbreak, fire, complex coordinated attack, or cyber incident) in order to control its impact and/or help prevent the occurrence of similar incidents.

Intelligence/Investigations Operations Center: A facility where I/I activities are managed and performed to support and assist the Intelligence/Investigations Section. If I/I activities continue after

the incident and resources at the incident site have been demobilized, the investigation may be managed exclusively at the I/I Operations Center.

intelligence requirement: The information and intelligence that must be collected and produced to eliminate intelligence gaps. Intelligence requirements convert intelligence gaps and the associated intelligence information needs into specific instructions regarding what information and intelligence to collect, report, produce, and disseminate. Intelligence requirements provide the questions that are asked of Human Intelligence sources and the information that is sought from Signals Intelligence, Imagery Intelligence, and Open-Source Intelligence. They are categorized as either standing or ad hoc intelligence requirements. Standing intelligence requirements are focused on significant intelligence gaps that require a sustained, long-term effort to resolve and are usually valid for years. Ad hoc intelligence requirements normally involve a particular investigation, incident, event, or activity and are normally valid for days or months.

international security/liaison community: Includes foreign government law enforcement, intelligence, and security agencies.

investigation: The systematic collection and analysis of information pertaining to factors suspected of contributing to, or having caused, an incident.

investigative evidence: Nonelectronic and electronic physical evidence that requires examination and evaluation but does not require scientific examination, analysis, comparison, and/or enhancement. Investigative evidence includes conventional, analog, and digital documents or text, images or photos, audio recordings, and data. Normally, one or more non-subject matter experts may perform the required examination and evaluation. However, based upon the facts and circumstances, one or more subject matter experts may have to perform the required examination and evaluation (e.g., accountant, translator, engineer, investigator, attorney, intelligence analyst, aircraft pilot, medical doctor, scientist, carpenter, or soldier).

investigative scene: An area or areas where investigative information may be obtained by identifying/interviewing witnesses, performing nontechnical and technical canvasses, examining conventional analog and digital investigative evidence (e.g., documents, images, audio recordings, or data), and using eyewitness identification techniques. Investigative scenes include:

- Casualty collection areas where ill/injured people are gathered for emergency triage, treatment, and/or transportation to a healthcare facility.
- Areas where decontamination operations are conducted.
- Fatality collection points where decedents are gathered for processing and safeguarding.
- Evacuation assembly areas or facilities.
- Shelter-in-place facilities or locations, when appropriate.

- Personnel checkpoints.
- Vehicle roadblocks.
- Traffic control points and access control points.
- Family Assistance Centers.
- Mass transit facilities or conveyances.
- Healthcare facilities, when appropriate.

mass fatality management: The performance of a series of activities including decontamination of decedent and personal effects (if required); determination of the nature and cause of death; identification of the fatalities using scientific means; certification of the cause and manner of death; processing and returning of decedents to the legally authorized people (if possible); and interaction with and provision of legal, customary, compassionate, and culturally competent services to the families of deceased within the context of the Family Assistance Center. All activities should be sufficiently documented for admissibility in criminal and civil courts. Mass fatality management activities are incorporated in the surveillance and intelligence sharing networks to identify sentinel cases of bioterrorism and other public health threats.

medical examiner: The official, in medical examiner jurisdictions, charged with the medicolegal investigation of deaths and fatality management. This individual is responsible for certifying the identification and determining the cause and manner of death. This individual has statutory jurisdiction over all bodies and decedents falling within the geographic jurisdiction and within certain prescribed categories of death. Mass fatality incidents may involve victims who are within those statutorily prescribed categories. Medical examiners are appointed officials. They are typically licensed medical physicians and can perform autopsies.

Medicolegal Death Investigation Authority: The legal authority in a jurisdiction to conduct operations, functions, and activities regarding death investigations. A medical examiner and/or coroner holds this authority.

missing person: A known individual being sought whose location is unknown, or an unidentified injured or deceased person.

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

multimedia evidence: Physical evidence consisting of analog or digital media, including film, tape, magnetic media, and optical media, and the information contained therein.

need to know: A determination made by an authorized holder of classified information that disclosure/dissemination of the information to an appropriately cleared individual is necessary to permit that individual to perform his/her official duties. The determination is not made solely by virtue of an individual's office, position, or security clearance level.

Nongovernmental Organization (NGO): An entity with an association that is based on interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with the government. Such organizations serve a public purpose, not a private benefit. Examples include faith-based charity organizations and the American Red Cross. NGOs, including voluntary and faith-based groups, provide relief services to sustain life, reduce physical and emotional distress, and promote the recovery of disaster victims. Often these groups provide specialized services that help individuals with disabilities. NGOs and voluntary organizations play a major role in assisting emergency managers before, during, and after an emergency.

nontechnical canvass: A traditional canvass for persons and vehicles to identify witnesses, sources of information, evidence, intelligence, leads, etc. Nontechnical canvasses may involve residential and commercial buildings, schools, recreational sites, mass transit facilities, crime scenes, and investigative scenes.

Open-Source Intelligence: Intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience to address a specific intelligence requirement.

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 security: A process to identify, control, and protect information that is generally available to the public regarding sensitive or classified information and activities that a potential adversary could use to the disadvantage of a governmental agency, NGO, or private entity/individual. Application of the operations security process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified information regarding the activities, capabilities, or intentions of a governmental agency, NGO, or private entity/individual.

The operations security process involves five steps:

1. Identify critical information: What must be protected?
2. Analyze the threat: Who is the potential adversary?
3. Analyze direct and indirect vulnerabilities: How might the adversary collect the information that must be protected?
4. Assess the risk: Balance the cost of correcting the vulnerabilities against the cost of losing the information that must be protected.

5. Implement appropriate countermeasures: Eliminate or reduce vulnerabilities, and/or disrupt the adversary's collection capabilities and efforts, and/or prevent the accurate interpretation of the information that must be protected.

On-Scene Security, Protection, and Law Enforcement (PPD-8, NPG, core capability): Ensure a safe and secure environment through law enforcement and related security and protection operations for people and communities located within affected areas and also for response personnel engaged in lifesaving and life-sustaining operations.

Operational Coordination (PPD-8, NPG, core capability): Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Planning (PPD-8, NPG, core capability): 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.

planned event: A scheduled nonemergency activity (e.g., sporting event, concert, parade).

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

private sector: Organizations and 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.

processing and exploitation: Converting raw information/data into formats that executives, managers, analysts, and investigators can efficiently and effectively use. Examples include:

- Imagery interpretation.
- Data conversion and correlation.
- Document and eavesdropping translations.
- Keyword searches on seized data.
- Facial recognition searches involving image capture systems, records, databases, etc.
- Data mining in seized or open-source databases.

- Decryption of seized or intercepted data.

production: The documentation and creation of finished and/or raw intelligence/information, which includes records, data, intelligence requirements, Intelligence Information Reports, warnings, reports, briefings, bulletins, biographies, and assessments in a conventional, analog, or digital format using text, images, audio, and data.

Public Information and Warning (PPD-8, NPG, core capability): 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, as well as the actions being taken and the assistance being made available, as appropriate.

request for information/intelligence: A means of submitting/transmitting one or more intelligence information needs to members of the U.S. Intelligence Community, law enforcement community, and Homeland Security community to be evaluated, validated (if applicable), assessed, deconflicted (if applicable), consolidated, prioritized, managed, and resolved.

sensitive compartmented information (SCI): A restricted access control system; a level of access to classified information compartments/programs, not a level of classification. The SCI access control system applies to all three levels of classified information (Top Secret, Secret, and Confidential). SCI access is usually based upon the sensitivity of the involved sources and/or methods.

Sensitive Compartmented Information Facility (SCIF): An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF.

Signals Intelligence: Intelligence information derived from the interception of transmitted electronic signals.

situation board: Large sheets of paper or whiteboards that are affixed to walls of the I/I Section work area and that are visible to those working an I/I operation. These boards give individuals immediate access to crucial information regarding the incident at hand. They also provide other I/I Section personnel a commanding view of information as it is processed.

staging area: Temporary location of available resources; it can be any location in which personnel, supplies, and equipment can be temporarily housed or parked while awaiting operational assignment.

tactical: Produced or implemented with only a limited or immediate objective.

tearline report: A report containing information that has been declassified or information that is at a reduced/downgraded classification level as compared to the original report from which the tearline

report is generated or produced. A tearline report is produced by redacting, paraphrasing, restating, or generating in a new form the classified information contained in the original report.

technical canvass: A canvass for electronic devices to identify witnesses, sources of information, evidence, intelligence, leads, etc. Technical canvasses may involve electronic image capture devices (e.g., still, video, closed-circuit television), electronic audio capture devices, electronic banking transaction devices (e.g., automated teller machine), electronic financial transaction devices (e.g., credit card, debit card, social services card, stored value card), electronic travel transaction devices (e.g., subway card, E-ZPass, airline ticket, railroad ticket), electronic access/egress control devices (e.g., identification card reader, proximity card reader, biometric card reader), cell sites, pay phones, and internet cafes.

Technical Specialist (THSP): Personnel with special skills that can be used anywhere within the ICS organization. No minimum qualifications are prescribed, as THSPs normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically certified in their fields or professions.

Unified Command (UC): An ICS application used when more than one agency has incident jurisdiction, or when incidents cross political jurisdictions. The use of UC enables multiple organizations to perform the functions of the IC jointly. Each participating partner maintains authority, responsibility, and accountability for its personnel and other resources while jointly managing and directing incident activities through the establishment of a common set of incident objectives, strategies, and a single IAP.

U.S. Intelligence Community: A coalition of agencies and organizations within the Executive Branch that work separately and together to gather the intelligence necessary for the conduct of foreign relations and the protection of the national security of the United States. The U.S. Intelligence Community functions as a single corporate enterprise, supporting those who manage the nation's strategic interests—political, economic, and military. The U.S. Intelligence Community comprises the following:

- Air Force Intelligence.
- Army Intelligence.
- Central Intelligence Agency.
- Coast Guard Intelligence.
- Defense Intelligence Agency.
- Department of Energy.
- Department of Homeland Security.

- Department of State.
- Department of the Treasury.
- Drug Enforcement Administration.
- Federal Bureau of Investigation.
- Marine Corps Intelligence.
- National Geospatial-Intelligence Agency.
- National Reconnaissance Office.
- National Security Agency.
- Navy Intelligence.
- Office of the Director of National Intelligence.

Appendix E. Resources

1. I/I Guidance Supporting Documents

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

1.1. National Incident Management System (NIMS)

- NIMS is a living document that evolves to capitalize on new opportunities and meet emerging challenges. Incident management stakeholders continue to build on this foundation by developing supporting tools, guidance, education, training, and other resources. Together, the components of NIMS enable nationwide unity of effort through shared vocabulary, systems, and processes to deliver the capabilities described in the National Preparedness System. NIMS concepts, principles, procedures, structures, and processes link the nation's responders together, enabling them to meet challenges beyond the capacity of any single jurisdiction or organization.

- https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf

1.2. Guideline for the Credentialing of Personnel

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

- https://www.fema.gov/emergency-managers/nims/components/nqs-supplemental-documents

1.3. ICS Resource Center

- The NIMS ICS Resource Center contains training courses, PTBs, job aids, and more to assist emergency response personnel in the use of ICS

- https://www.fema.gov/incident-command-system-resources

1.4. NIMS Resource Center

- The NIMS website contains links to several supporting guides and tools for NIMS implementation. As FEMA develops new items, they will be added to this site.

- https://www.fema.gov/national-incident-management-system

1.5. NIMS Training Program

- This resource supersedes the previous training guidance, the Five-Year NIMS Training Program.
- The NIMS Training Program specifies FEMA and stakeholder responsibilities and activities for developing, maintaining, and sustaining NIMS training. The NIMS Training Program outlines responsibilities and activities that are consistent with the National Training Program, as mandated by the Post-Katrina Emergency Management Reform Act (PKEMRA) of 2006.
- https://www.fema.gov/emergency-managers/national-preparedness/training

2. Relevant Law

2.1. Homeland Security Act of 2002

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

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

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

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

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

2.4. Robert T. Stafford Disaster Relief and Emergency Assistance Act

- The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. 100-707, signed into law Nov. 23, 1988, amends the Disaster Relief Act of 1974, Pub. L. 93-288. The Stafford Act

constitutes the statutory authority for most federal disaster response activities, especially as they pertain to FEMA and FEMA programs.

- http://www.fema.gov/robert-t-stafford-disaster-relief-and-emergency-assistance-act-public-law-93-288-amended

2.5. Sandy Recovery Improvement Act of 2013

- The Sandy Recovery Improvement Act of 2013 became law on Jan. 29, 2013, and amends the Robert T. Stafford Disaster Relief and Emergency Assistance Act. This Act authorizes changes to the way FEMA delivers federal disaster assistance, with the goals of (1) reducing the costs to the federal government of providing such assistance; (2) increasing flexibility in the administration of assistance; (3) expediting the provision of assistance to a state, tribal, or local government, or owner or operator of a private nonprofit facility; and (4) providing financial incentives and disincentives for the timely and cost-effective completion of projects.

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

3. Additional Supporting Materials

Additional supporting materials include:

3.1. Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining Emergency Operations Plans, Version 3

- Published in 2021, FEMA's CPG 101, Version 3.0 provides guidance on the fundamentals of planning and development of emergency operations plans (EOP) CPG 101, Version 3.0 encourages emergency and homeland security managers to engage the whole community in addressing the risks that potentially impact their jurisdictions.

- https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf

3.2. Considerations for Fusion Center and Emergency Operations Center Coordination

- EOCs should have awareness of Fusion Center roles and capabilities to facilitate successful coordination

- Considerations for Fusion Center and Emergency Operations Center Coordination

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

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

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

3.4. Emergency Management Assistance Compact (EMAC)

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

- http://www.emacweb.org/

3.5. Federal Interagency Operational Plans (FIOP)

- The Federal Interagency Operational Plans (FIOP) describe how the federal government aligns resources and delivers core capabilities to implement the five National Planning Frameworks. The FIOPs provide a federal concept of operations, integrating and synchronizing national-level capabilities for the five mission areas (Prevention, Protection, Mitigation, Response, and Recovery) to support all levels of government. These plans also help federal departments and agencies develop and maintain department-level operational plans.

    - Prevention Federal Interagency Operational Plan.[33]

    - Protection Federal Interagency Operational Plan, August 2016.

    - Mitigation Federal Interagency Operational Plan, August 2016.

    - Response and Recovery Federal Interagency Operational Plan, March 2023.

[33] This plan contains sensitive information and is not publicly available on unclassified systems in the interest of national security. Stakeholders who would like a copy may receive one through their local fusion center or by emailing FEMA at PPD8-NationalPreparedness@fema.dhs.gov.

- https://www.fema.gov/emergency-managers/national-preparedness/frameworks/federal-interagency-operational-plans

3.6. National Emergency Communications Plan (NECP)

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

3.7. National Information Exchange Model

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

3.8. National Planning Frameworks

- The National Planning Frameworks, one for each mission area, describe how the whole community works together to achieve the NPG:
  - National Prevention Framework, Second Edition, June 2016.
  - National Protection Framework, Second Edition, June 2016.
  - National Mitigation Framework, Second Edition, June 2016.
  - National Response Framework, Fourth Edition, October 2019.
  - National Disaster Recovery Framework, Second Edition, June 2016.
- https://www.fema.gov/emergency-managers/national-preparedness/frameworks

3.9. National Preparedness Goal (NPG)

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

3.10. National Preparedness System

- The National Preparedness System outlines an organized process for everyone in the whole community to move forward with their preparedness activities and achieve the NPG.

- http://www.fema.gov/national-preparedness-system

3.11. National Wildfire Coordinating Group (NWCG)

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

- http://www.nwcg.gov/

3.12. NIMS Basic Guidance for Public Information Officers

- The NIMS Basic Guidance for Public Information Officers provides fundamental guidance for any person or group with PIO responsibilities. The document addresses actions for command and coordination, preparedness, incident response, strategic communication, incident recovery, and digital communication. The guidance material is adaptable to individual jurisdictions and specific incident conditions.

- https://www.fema.gov/sites/default/files/documents/fema_nims-basic-guidance-public-information-officers_12-2020.pdf

3.13. IMS Guideline for Resource Management Preparedness

- Published in 2021, the NIMS Guideline for Resource Management Preparedness supplements the NIMS Resource Management component by providing additional details on processes, best practices, authorities, and tools. The audience for this guide is any AHJ that is responsible for acquiring, inventorying, storing, or sharing resources. Whether building a new resource management program or working to improve an existing one, AHJs can use this guide to find information about resource management preparedness and best practices.

- https://www.fema.gov/sites/default/files/documents/nims-guideline-resource-management-preparedness.pdf

3.14. Presidential Policy Directive / PPD-8: National Preparedness

- Published in March 2011, PPD-8 is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyberattacks, pandemics, and catastrophic natural disasters.

- https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

3.15. Resource Inventory System (RIS)

- RIS is FEMA's centralized, secure, cloud-hosted resource inventory solution. It is provided at no cost to local, state, tribal, territorial, and federal agencies as well as NGOs and other partners. RIS enables users to identify and inventory their resources consistently with NIMS resource typing definitions and National Qualification System (NQS) positions. The tool can be used to inventory equipment, personnel, teams, facilities, and supplies.

- https://preptoolkit.fema.gov/web/national-resource-hub/resourceinventorying

3.16. Resource Management and Mutual Aid Guidance

- Resource management guidance and tools support the use of consistent resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.

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

3.17. Resource Typing Library Tool (RTLT)

- FEMA's RTLT is an online catalog of national resource typing definitions and job titles/position qualifications. Definitions and job titles/position qualifications are easily searchable through the RTLT.

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

3.18. United States Coast Guard (USCG)

- The Coast Guard uses NIMS guidance extensively. USCG efforts have helped to extend the NIMS audience by institutionalizing the use of ICS for all incidents, including spills and security operations.

- http://www.uscg.mil/

3.19. Using Social Media for Enhanced Situational Awareness and Decision Support

- Published in 2014, this DHS report provides examples of how organizations can use social media to enhance situational awareness and support operational decision-making, as well as challenges and potential applications.

- https://www.dhs.gov/publication/using-social-media-enhanced-situational-awareness-decision-support