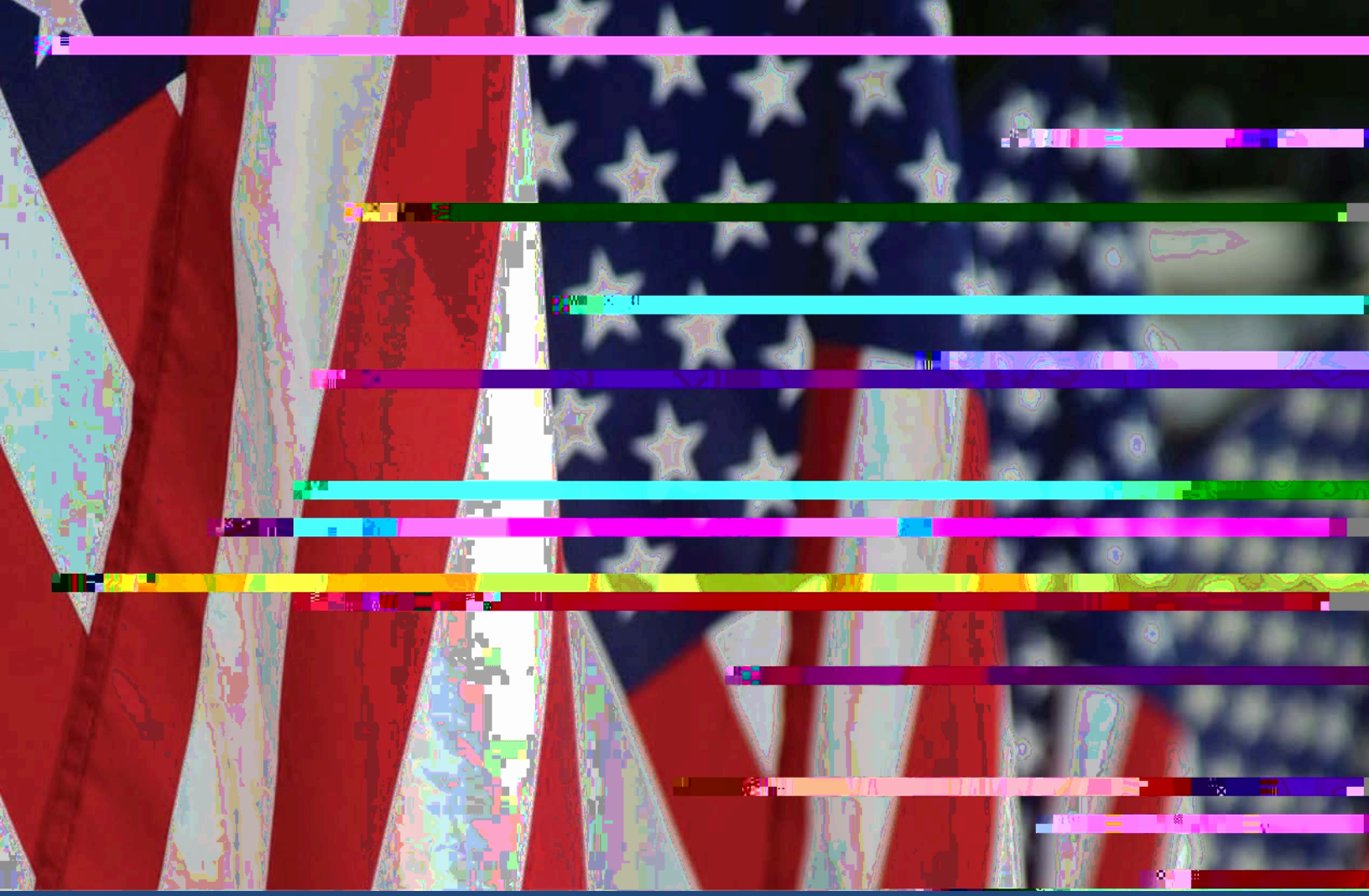

NATIONAL INCIDENT MANAGEMENT SYSTEM

Intelligence/Investigations Function Guidance and Field Operations Guide

October 2013

Homeland Security

Table of Contents

This page intentionally left blank.

Intelligence/Investigations Function Guidance

The National Incident Management System (NIMS) represents a core set of doctrine, concepts, principles, terminology, and organizational processes that enables effective, efficient, and

or complexity.[2] The activities and information that are at the core of the I/I Function have historically been viewed as the primary responsibilities of "traditional" law enforcement departments and agencies at all levels of government. Although, in many cases, law enforcement departments/agencies fulfill intelligence/investigations duties, the I/I Function has aspects that cross disciplines and levels of government. "Nontraditional" forms of intelligence/investigations activities (i.e., non-law enforcement) might include:

Epidemiology

Mass fatality management

Fire, explosion, or arson cause and origin (regardless of likelihood of criminal activity)

Real-time research and analysis intended to protect against, respond, and/or recover from a specific incident (e.g., critical infrastructure vulnerability and consequence analysis; hurricane forecast regarding strength and estimated point of landfall; post-earthquake technical clearinghouse; or post-alert volcanic monitoring)

Transportation accidents.

This document can be used by jurisdictions and agencies when developing new plans for establishing the I/I Function or when incorporating the I/I Function into existing plans. Users of this document are encouraged to tailor its content, including the information and model in the I/I FFOG, to reflect jurisdiction authorities and/or incident needs.

This document contains a recommended organizational framework for executing the I/I Function. The I/I Guide provides neither legal authority nor direction and does not supersede applicable legal authorities and constraints at any jurisdictional level. Personnel managing and performing intelligence and investigations activities must always comply with applicable authorities, statutes, law, ordinances, regulations, and policies within and affecting their jurisdiction and/or agency. This document informs Command and General Staff personnel who are responsible for making strategic and operational decisions during an incident. The guidance provided in this document does not empower or authorize personnel to take on roles or responsibilities for which they are not authorized, trained, or certified, nor does it substitute for training in the proper tactics, techniques, and procedures related to performing intelligence- and investigations-related operations functions and activities. Users should consult their agency counsel to determine applicable authorities.

Additionally, intelligence and investigations practitioners must protect constitutional, victim, and privacy rights, civil rights, and civil liberties; restrict the dissemination of sensitive/classified information; and honor legally imposed restrictions on investigative behavior that affect the admissibility of evidence and the credibility of witnesses.

[2] Intelligence gathered within the I/I Function is information that either leads to the detection, prevention, apprehension, and prosecution of criminal activities, or the individuals involved, including terrorist incidents or information that leads to determination of the cause of a given incident (regardless of the source), such as public health events or fires with unknown origins. (Federal Emergency Management Agency, National Incident Management System, December 2008)

Introduction

NIMS provides a systematic, proactive approach guiding local, state, tribal, territorial, insular area, and Federal governments; the private sector; and nongovernmental organizations to work seamlessly to prevent, protect against, mitigate, respond to, and recover from the effects all threats and hazards. NIMS is based on the premise that the use of a common incident management framework provides emergency management and response personnel a standardized system for emergency management and incident response activities.

Presidential Policy Directive (PPD) 8 describes the Nation's approach to national preparedness. The National Preparedness Goal is the cornerstone for the implementation of PPD-8; identified within it are the Nation's core capabilities across five mission areas: Prevention, Protection, Mitigation, Response, and Recovery. The National Preparedness System is the instrument employed to build, sustain, and deliver those core capabilities in order to achieve the goal of a secure and resilient Nation. The National Planning Frameworks, which are part of the National Preparedness System, set the strategy and doctrine for building, sustaining, and delivering the core capabilities. The maturation and use of NIMS helps ensure that a unified approach across all mission areas as the National Preparedness System is implemented.

Pursuant to NIMS, a single set of objectives is developed for the entire incident, and a collective approach is used to develop strategies to achieve incident objectives. All agencies with responsibility for the incident have an understanding of joint priorities and restrictions, and no agency's legal authorities are compromised or neglected. The combined efforts of all agencies are optimized as they perform their respective assignments under a single Incident Action Plan (IAP).

Most incidents are managed locally and typically do not need

Security Information Network (HSIN),[6] RISS,[7] Law Enforcement Online (LEO),[8] 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

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

- Prevent/Deter 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 intelligence/investigations operations being initiated concurrently. The IC/UC ensures that provisions are made for the safety, health, and security of responders and that intelligence/investigations operations contribute toward a safer, healthier, and more secure life safety operation.

In today's multi-hazard and threat environment, response personnel should consider all potential causes of an incident (e.g., accidental, criminal, or natural) and take the necessary steps to preserve potential evidence and/or crime scenes while protecting life safety. To efficiently and effectively develop and use intelligence/investigations information, the I/I Function is integrated into the ICS structure. The ICS allows for scalability and the IC/UC has the flexibility to establish the I/I Function within the incident management organizational structure based upon the nature and type of incident.

The I/I Function should be established as a General Staff Section when a criminal or terrorist act is involved. 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 and may establish task force operations for crime scene processing. 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 life safety of the responders and/or the public, the information can and should be shared with appropriate Command and General Staff.

Life safety is always the primary incident objective. The establishment of the I/I Function as a General Staff Section does not diminish or alter this primary objective in any way. It enhances the primacy of the life safety incident objective. For example, evidence recovered from the incident scene and the information produced from the intelligence/investigations activities may prevent a subsequent criminal or terrorist act from occurring at the incident site or at other locations.

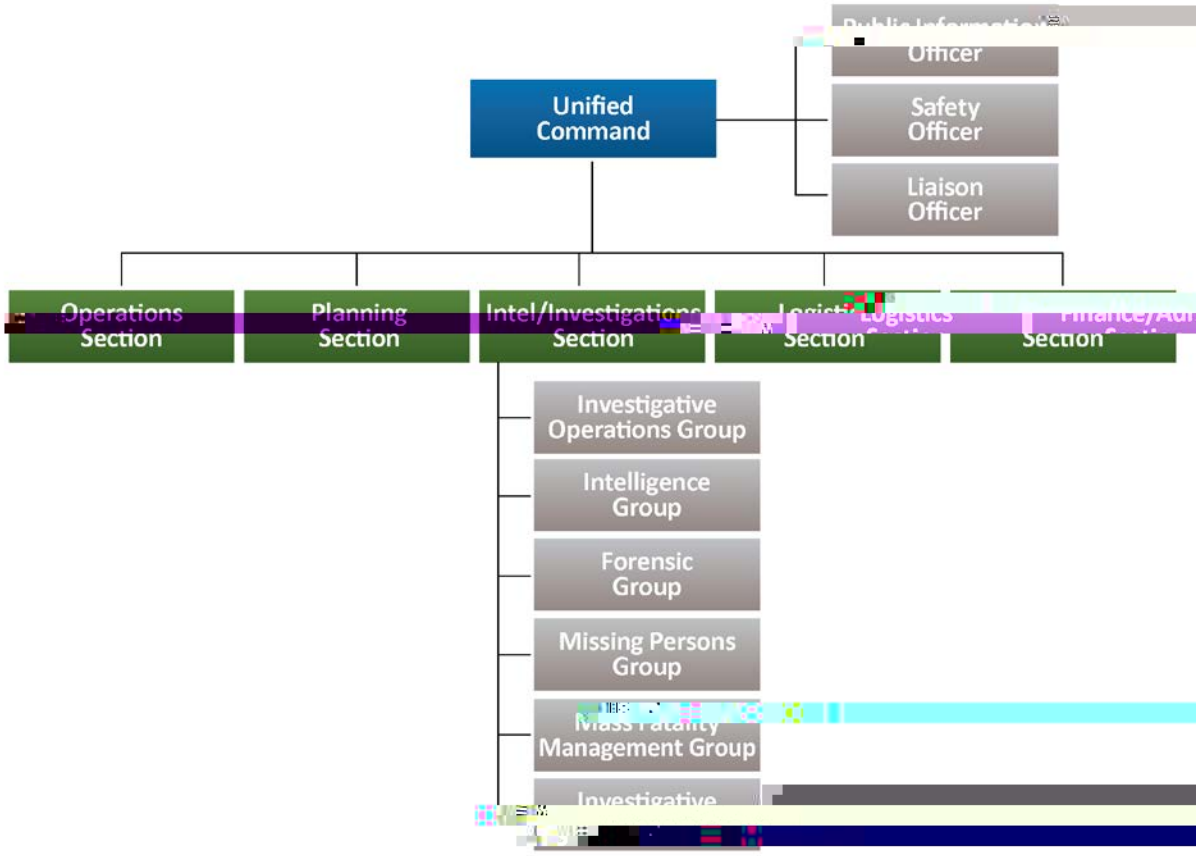

Figure 2: Intelligence/Investigations as a General Staff Section

The Groups are discussed further in the I/I FFOG.

In specific instances, the work of the I/I Section may be performed by an extremely large number of personnel. Span of control problems due to a large number of personnel should be prevented or resolved (i.e., the Section is too large to support the direct reporting of Groups to the Section Chief). In this case or when other appropriate circumstances exist, the I/I Section Chief may activate one or more Branches within the I/I Section instead of one or more Groups and designate a Branch Director for each activated Branch. The Branches that may be activated are:

Investigative Operations Branch

Intelligence Branch

Forensic Branch

Missing Persons Branch

Mass Fatality Management Branch

Investigative Support Branch.

The I/I Function within ICS provides a flexible and scalable framework that allows for the

Intelligence/Investigations Function Field Operations Guide

The I/I FFOG assists those implementing the I/I Function as a Section within an incident command structure during incidents or planned events, regardless of type, cause, size, location, or complexity. The I/I FFOG describes the I/I Function as a General Staff Section to illustrate the potential tasks and responsibilities within the I/I Section.

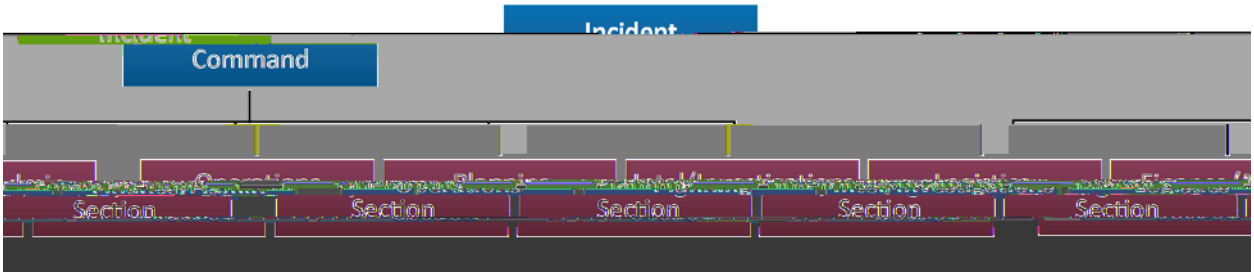

Figure 3: Intelligence/Investigations as a General Staff Section

The I/I FFOG does not replace emergency operations plans, laws, regulations, or ordinances. Rather, it provides guidance for personnel assigned to an incident or planned event. The information contained in the I/I FFOG supplements the user's experience, training, and knowledge in the performance of intelligence/investigations activities. It also provides a model for organizing and managing intelligence/investigations operations and activities.

The contents of this I/I FFOG are not a substitute for required formal training, intelligence/ investigations operations experience, and good judgment. Personnel using the I/I FFOG 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 (mass fatality), the National Transportation Safety Board (transportation incidents), and the Environmental Protection Agency (oil spills). No matter what the nature or type of incident, personnel managing and performing intelligence/investigations 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 intelligence/investigations 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

The I/I FFOG 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 FFOG 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.

Initial Setup

The 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/or 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 regarding the I/I Section and ensure that incident personnel are promptly notified.

Confer with the IC/UC to determine those intelligence/investigations agencies that are involved in the incident. The involvement of some agencies may be required by law.

Ensure that:

- Intelligence/investigations activities are expeditiously implemented. Intelligence/ Investigations activities may be initiated concurrently with life safety operations; absent extraordinary emergency circumstances, life safety operations incident objectives 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 Technical Specialist is assigned to the I/I Section work area
- A

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.

Responsibilities

The role of the Deputy I/I Section Chief is flexible, and the 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 intelligence/investigations-related activities, resources, services, support, and reserves
- The implementation and effectiveness of the documented intelligence/ investigations objectives, strategies, and priorities and the intelligence/investigations 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 intelligence/investigations-related requirements and problems

Maintain situational awareness for the I/I Section Chief

Ensure that the Public Information Officer assists with public affairs and media-related

- The intelligence/investigations aspects and components of the Demobilization Plan
- Documentation and records management procedures, measures, and activities.

Ensure that:

- Intelligence/investigations needs are considered when the 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.

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 both the internal and external logistics/communications efforts of the I/I Section.

Internal Tasks/Responsibilities

Resource Management

Intelligence/Investigations 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

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 a result of both the sensitive nature of intelligence/ investigations 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 remains, as well as manages, coordinates, and directs all of the intelligence/ investigations operations, functions, and activities.

Considerations to remember as the I/I Section work area location is being selected and maintained include:

Establishing the I/I Section work area at a secure location a reasonable distance from the O10(as)>e8(ect)ons, 6]TJ 0 Tc 0 T 0.00492(or)6dEd(t)- S, aa66]6(s)-5(al)-6(l)-6(o)-1301(an)-3w -6.0(W(

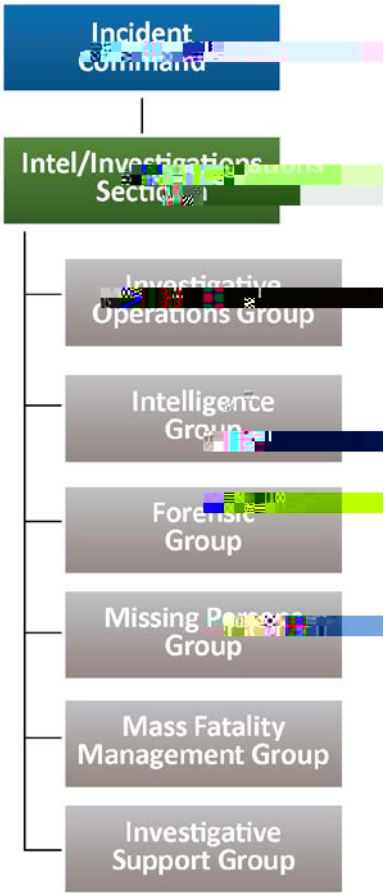

Figure 4: Intelligence/Investigations Section Organization

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 of 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 intelligence/investigations 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 of the associated materials are invoiced, safeguarded, and examined

All forensic evidence, digital and multimedia evidence, and investigative evidence (e.g., documents, images, audios, and data) are invoiced, safeguarded, and analyzed

All investigative reports and materials associated with the results of each assigned investigative lead/task and the related forensic, investigative, and digital and multimedia evidence 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)

Acquisition and analysis of records and other evidence

Polygraph examinations

Undercover officer and confidential informant operations

Activation and use of tiplines, hotlines, and/or call centers

Dissemination of alarms, "Be on the Lookout" messages, alerts, warnings, and notices

Obtaining and securing of sources of investigatory data, such as flight data recorders, cockpit voice recorders, vehicle electronic data recorders, radar data, and 9-1-1 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

Tactical Operations Coordinator.

Intelligence Group

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

The information intake and assessment function ensures that incoming information, except the results of investigative leads/tasks, is:

Communicated directly to the Intelligence Group

Documented on an information control form and/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 being 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)

- Classified information and/or access-controlled sensitive compartmented information and/or caveated/restricted information is sanitized to use the information to create and investigate leads/tasks, publish intelligence products, prepare warrant applications and accusatory instruments, etc.
- Intelligence/investigations 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 intelligence/investigations information

When applicable, ensuring that requests for intelligence/investigations information are documented, analyzed, managed, and resolved

Conferring with the Planning Section regarding information/intelligence-related activities as needed.

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 doi coiyP1 T

Bomb Operations Coordinator

Chemical, Biological, Radiological, Nuclear/Hazardous Materials

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, dissemination, etc., activities are implemented
- When necessary, Disaster Mortuary Operational Response Teams or other similar resources are requested
- When necessary, debris sifting operations are implemented
- All of the 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 medical examiner/coroner expeditiously determines the cause and manner of death of each of the decedents and the final disposition of each of the decedents
- The appropriate authority expeditiously issues a death certificate regarding each of the decedents
- Required information, data, records, images, DNA reference samples, investigative evidence, forensic evidence, digital/multimedia evidence, and non-evidence property regarding decedents are obtained at one or more Family Assistance Centers and/or appropriate facilities/areas.

Depending upon the size, complexity, and scope of the I/I Section, the Mass Fatality Management Group Supervisor may activate one or more of 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.

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 Staffs, 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 and each staging area is situated at an appropriate location; a Staging Area Manager is designated for each of the activated staging areas

- Resources are tracked.

Intelligence/Investigations Section Work Area Manager

- Ensure that the I/I Section work area is maintained in an orderly manner.
- In coordination with the Logistics Section, ensure 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

- If a significant number of intelligence/investigations resources are required, work directly with counterparts in the Logistics Section to order the resources and in the Planning Section to account for all resources.
- Ensure 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 or replaced when necessary; safeguarded; tracked; documented; properly 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

- This position works directly with the Logistics Section.
- Ensure 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 or replaced when necessary, safeguarded, appropriately distributed, tracked, documented, properly 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.
- Ascertain the designated “system” radio channels and “point-to-point” radio channels that are being used for the incident.
- Designate the I/I Section “system” radio channels and “point-to-point” radio channels as needed.

List of Abbreviations and Glossary of Key Terms

List of Abbreviations

EMR–ISAC	Emergency Management and Response–Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
HSIN	

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 (Confidential, Secret, or Top Secret) 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, 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 as required. They may have an assistant or assistants, as needed.

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 and decedents. This individual has statutory jurisdiction over all bodies and decedents falling within the geographic jurisdiction and within certain prescribed categories of death.

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

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

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

Incident 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 Security: The policies, practices, and procedures that ensure that information/intelligence stored, processed, transmitted, etc., using information technology systems and networks is secure, and not vulnerable to inappropriate or unauthorized discovery, access, export, use, modification, etc.

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 agency-wide 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 Gap: An unanswered question regarding a criminal, cyber, or national security

Law Enforcement Community. Analysts use Intelligence Information Reports and other available sources of information/intelligence to produce "finished" information/intelligence.

Intelligence/Investigations Operations Center: Intelligence/Investigations activities are managed and performed at the Intelligence/Investigations Operations Center to support and assist the Intelligence/Investigations Section. Furthermore, if intelligence/investigations activities continue after the incident and resources at the incident site have been demobilized, the investigation may be managed exclusively at the Intelligence/Investigations Operations Center.

Intelligence Requirement: The information and/or 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

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: Personnel with special skills that can be used anywhere within the Incident Command System organization. No minimum qualifications are prescribed, as technical specialists normally perform the same duties during an incident that they perform in their everyday jobs, and they are typically certified in their fields or professions.

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

This page intentionally left blank.