



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

MEMORANDUM FOR: NIMS Stakeholders

FROM: Al Fluman
Acting Director, National Integration Center, Incident
Management Systems Integration Division

SUBJECT: National Comment Period on the NIMS Draft
Intelligence/Investigations Function Guidance Document and Field
Operations Guide

As part of our Nation's efforts to expand the National Incident Management System (NIMS), the Incident Management Systems Integration Division has developed a Draft NIMS Intelligence/Investigations Function Guidance Document and Field Operations Guide (FOG) to assist emergency responders to efficiently and effectively prevent, protect against, respond to, recover from and mitigate the effects of incidents.

The revised NIMS document (draft available: <http://www.fema.gov/emergency/nrf/mainindex.htm#>) included the Intelligence/Investigations Function as an optional sixth functional area that is activated on a case-by-case basis. The purpose of the document is to further define the roles and responsibilities within this Function. The attached draft document contains two distinct sections. The first includes general guidance that expands upon the information currently found within the revised NIMS document, and the second is a draft Intelligence/Investigations Function FOG.

As part of the review process, stakeholders may participate in a 30-day comment period (**February 25 - March 26, 2008**). To submit comments on the Draft NIMS Intelligence/Investigations Function Guidance Document and FOG, email comments to NIMScomments@hsi.dhs.gov OR send an email to request a comment form. Submissions using this form are NOT required but will help ensure clarity and continuity during the comment adjudication process.

1

2

3

4

INTELLIGENCE/INVESTIGATIONS FUNCTION GUIDANCE DOCUMENT

5

Version 3

6

February 2008

7

8

9

10

11

12

13

14

15

16

Commenting on the Draft Document:

If you would like to submit comments on this document email your comments to NIMScments@hsi.dhs.gov OR send an email to request a comment form. Submitting comments using this form is NOT required but will help assure clarity and continuity during the comment adjudication process.

1 **Table of Contents**

2

3 Table of Contents i

4 Purpose..... 1

5 Introduction..... 2

6 Intelligence/Investigations Function..... 5

7 Potential Placement of Intelligence/Investigations Function within ICS Structure..... 5

8 Maintaining Linkages between Intelligence/Investigations Section and Incident Command

9 Structure 11

10 Organizational Connectivity and Deconfliction 12

11 Use and Organization of Groups..... 13

12 Use and Organization of Branches 14

13 Summary 15

14 Intelligence/Investigations Function Field Operations Guide 16

15 Purpose and Organization 16

16 Intelligence/Investigations Functional Overview 17

17 Initial Setup..... 17

18 Use of Deputies..... 19

19 Internal/External Intelligence/Investigations Activities and Relationships 20

20 Intelligence/Investigations Physical Location and Work Area..... 23

21 Groups and Structure within the Intelligence/Investigations Section..... 25

22 Investigative Operations Group 25

23 Intelligence Group 27

24 Forensic Group..... 29

25 Medicolegal Group 30

26 Investigative Support Group..... 30

27 Acronym List 33

28 Definitions..... 34

Purpose

The events of September 11, 2001, highlighted the importance of sharing information and intelligence, which has become integral to preventing or mitigating future tragedies. The goal of sharing information and intelligence is to develop a common operating picture for all emergency management/response personnel. The Intelligence/Investigations Function within the Incident Command System (ICS) provides a flexible and scalable framework that will allow for the integration of intelligence and investigations activities and information.¹

This document will provide guidance on how to utilize and integrate this Function while adhering to the concepts and principles of the National Incident Management System (NIMS). It will present information intended for the ICS practitioner (including the Incident Commander/Unified Command) that will assist in the decision-making process regarding the placement of the Function within the command structure and will provide tools that may be used while implementing the Function. While there is no one-size-fits-all approach to establishing this Function, the information contained in this document should provide helpful points of reference.

This Guidance and the accompanying Intelligence/Investigations Field Operations Guide (IIFOG) are applicable in all situations involving intelligence/investigations information ranging from every-day operations which utilize conventional unclassified information (e.g., criminal histories, medical records, educational records) up to terrorist incidents where the information is classified to the highest levels and requires the incorporation of National intelligence capabilities provided by the U.S. Intelligence Community assets.

To assist in maintaining a flexible but standardized system, it is necessary to develop guidance for the Function. Like all aspects of ICS, the Intelligence/Investigations Function may be operated by personnel representing various disciplines, this document, therefore, seeks to inform the Command and General Staff personnel who are responsible for making strategic decisions during an incident. *This document, however, does not act as a substitute for training in the tactics or actions related to performing intelligence/investigations related operations, functions and activities.*

The activities and information that are at the core of this Function are often viewed as primary responsibilities of “traditional” law enforcement. In many cases, intelligence/investigations duties are fulfilled by law enforcement department/agencies; but this Function has aspects that cross disciplines. “Non-traditional,” non-law enforcement forms of investigation might include epidemiological investigations, regulatory investigations, medical examiner/coroner (ME/C) investigations as well as those conducted by the National Transportation Safety Board or other investigatory agencies. Moreover, this Function can be utilized for planned events, as well as incidents.

¹ Defined as information that either leads to the detection, prevention, apprehension, and prosecution of criminal activities (or the individual(s) involved) including terrorist incidents or information that leads to determination of the cause of a given incident (regardless of source) such as public health events or fires with unknown origins.

1 Introduction

2
3 NIMS provides a systematic, proactive approach guiding Federal, State, Tribal and local
4 governments, the private sector, and nongovernmental organizations to work seamlessly to
5 prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of
6 cause, size, location, or complexity, in order to reduce the loss of life, property, and harm to the
7 environment. NIMS is based on the premise that the utilization of a common incident
8 management framework will give emergency management/response personnel a flexible and
9 scalable, yet standardized, system for emergency management and incident response activities.
10 These principles are echoed throughout the components of NIMS.

11
12 Summarized below is an overview of how the Intelligence/Investigations Function is
13 incorporated into each NIMS component.

14
15 Preparedness: Preparedness includes the following elements: planning, procedures and
16 protocols, training and exercises, personnel qualifications and certification, and
17 equipment certification. The Intelligence/Investigations Function can be used to provide
18 intelligence/investigations information to planners in order to ensure that planning
19 activities address all possible contingencies. The Function is important when planning
20 for events (such as large conventions, sporting events or National Special Security
21 Events) as it fosters information sharing and collaboration. Training and exercising on
22 the Intelligence/Investigations Function in advance of an incident and incorporating the
23 Function into planning efforts will facilitate efficient emergency management and
24 incident response activities. It is vital to prepare for the possibility that an incident may
25 escalate beyond the resources of a local community or that an investigation may continue
26 past initial response. Preparedness activities should incorporate the possibility that
27 Federal Government assets may be needed and should include contingencies for the
28 possibility that an incident may be caused by terrorism which may necessitate increased
29 coordination with the Federal Government.

30
31 Communications and Information Management: Effective emergency management and
32 incident response activities rely upon flexible communications and information systems
33 to provide a common operating picture to emergency management/response personnel.
34 Planning for communications and information management must address the policies and
35 procedures, equipment, systems, standards, and training necessary to achieve integrated
36 communications. Of particular importance to the Intelligence/Investigations Function is
37 having information management systems in place, as well as having the means necessary
38 to safeguard information (e.g., operations security protocols). Important aspects of
39 information management include the identification of and familiarization with
40 communications systems, tools, procedures and methods. The Function works to ensure
41 that necessary types of information (including, but not limited to, voice, data, image, text)
42 are shared amongst appropriate personnel (i.e., persons with appropriate clearance,
43 access, need-to-know).

44
45 Resource Management: Resource management involves the coordination, oversight, and
46 processes that provide timely and appropriate resources during an incident. Ensuring that

1 the proper resource management systems and procedures are in place prior to an incident
2 (or a planned event) is crucial in order to acquire the resources necessary during an
3 incident. Resource management is integral to intelligence/investigations activities as a
4 means of providing logistical support, credentialing personnel prior to incidents, and
5 badging of emergency management and incident response personnel during incidents.
6

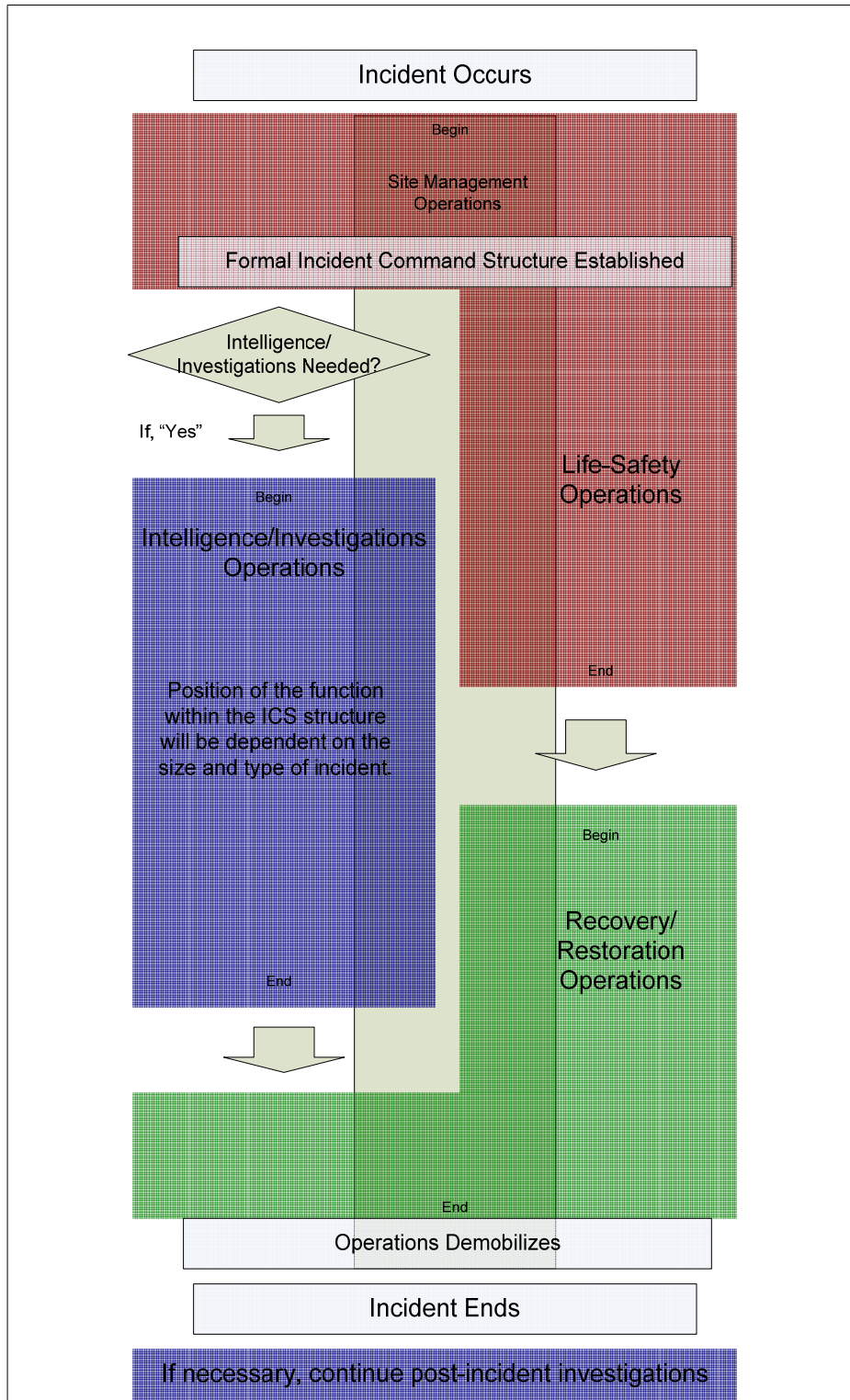
7 Command and Management: The Incident Command System (ICS), Multiagency
8 Coordination Systems (MACS), and Public Information are the fundamental elements of
9 incident management. These elements provide standardization through consistent
10 terminology and established organizational structures. The collection, analysis, and
11 sharing of incident-related intelligence are aspects of ICS. The
12 Intelligence/Investigations Function provides several crucial benefits to an Incident
13 Commander/Unified Command (IC/UC), including, but not limited to the following:

- 14 1. Provides an IC/UC with classified information, Sensitive Compartmented
15 Information and Sensitive Information in the same manner as these types of
16 information would be made available to Federal government personnel who may be
17 responding to the incident.
- 18 2. Allows an IC/UC to initiate Intelligence/Investigations operations concurrently with
19 life safety operations in order to protect evidence at crime and investigative scenes
20 while ensuring that life safety operations remain the primary incident objective (See
21 chart 1, page 4).
- 22 3. Allows an IC/UC to determine whether the incident is the result of criminal acts or
23 terrorism, and to maximize efforts to prevent additional criminal activities or
24 terrorism.
- 25 4. When appropriate, provides a means of linking directly to the Federal Bureau of
26 Investigation's (FBI) Joint Operations Center (JOC) to provide for constant
27 information-sharing to ensure that operational activities undertaken by varying
28 agencies are not in conflict (e.g., crime scene processing, interviewing witnesses,
29 physical surveillance), and affords coordination with other information-sharing
30 entities including Regional Fusion Centers, Regional Intelligence Sharing
31 Consortiums and the National Counter Terrorism Center.
- 32 5. Ensures that an IC/UC has the appropriate personnel with the necessary subject
33 matter expertise to conduct the required intelligence/investigative operations.
34

35 ICS is designed to enable effective and efficient incident management by integrating a
36 combination of facilities, equipment, personnel, procedures and communications operating
37 within a common organizational structure. The flexibility of ICS allows it to be used by all
38 levels of government—Federal, State, Tribal, and local—as well as by many private sector and
39 nongovernmental organizations, and is also applicable across multiple disciplines. Normally
40 structured to facilitate activities in five major functional areas: Command, Operations, Planning,
41 Logistics, and Finance/Administration, ICS can be expanded to include a sixth optional
42 functional area, Intelligence/Investigations, on a case-by-case basis. The diagram on the
43 following page depicts the flow of events in establishing the Intelligence/Investigations Function.

1
2

Chart 1: Flow of Events in Establishing Intelligence/Investigations Function



3

1 **Intelligence/Investigations Function**

2
3 The mission of the Intelligence/Investigations Function² is to ensure that all
4 intelligence/investigations operations and activities are managed, coordinated, and directed in
5 order to:

- 6
- 7 • Prevent/deter potential unlawful activity, incidents, and/or attacks
 - 8 • Collect, process, analyze, safeguard, and appropriately disseminate intelligence information
 - 9 • Conduct a thorough and comprehensive investigation
 - 10 • Identify, document, process, collect, create a chain of custody for, safeguard,
11 examine/analyze, and store probative evidence
- 12

13 In order to accomplish the mission of the Function, the IC/UC must determine the incident
14 objectives and strategies and then prioritize them. These priorities may shift as an incident
15 changes. Ultimately, life safety operations are the highest priority, though
16 intelligence/investigations operations may be initiated concurrently. It is the IC/UC's
17 responsibility to ensure that provisions are made for the safety, security and health of responders.
18

19 In today's threat environment, a mindset must be fostered among response personnel
20 encouraging them to consider all potential causes of an incident [accidental, intentional
21 (including terrorism), or naturally occurring]. This mindset should encourage the preservation of
22 potential evidence and/or crime scenes and also encourage the use of US Intelligence
23 Community assets and capabilities (e.g., Central Intelligence Agency, National Security Agency,
24 Department of Defense). In order to efficiently and effectively develop and utilize
25 intelligence/investigations information, an Intelligence/Investigations Function should be
26 integrated into ICS. As ICS allows for organizational flexibility and scalability, the Function can
27 be embedded in several ways within the Command structure.

28 **Potential Placement of Intelligence/Investigations Function within ICS** 29 **Structure**

30
31 The Intelligence/Investigations Function provides the IC/UC with the flexibility to adapt the role
32 of the Function in response to incident needs. As the need to handle intelligence/investigations
33 operations varies within an incident or between different types of incidents, so will the location
34 of the Function within the command structure. A fully activated Intelligence/Investigations
35 Function may be appropriate when there is a significant intelligence/investigations component to
36 an incident (e.g., for incidents with criminal or epidemiological elements or when multiple

² Though similar in some areas, it should be noted that the Intelligence/Investigations Function is not meant to supplant or compete with the activities implicit in the Planning Section, or oversee operational or situational intelligence (e.g., situation status, resource status and anticipated incident status). The situational and resources functions within the Planning Section focus on incident-wide issues, while the Intelligence/Investigations Function deals with development of information and/or evidence that will focus on potentially criminal aspects of the incident, with public health investigations into epidemiology, or with the complex activities related to the handling of mass fatality situations, etc.

1 investigative agencies are involved and resources require the establishment of appropriate
2 supervision). A separate Intelligence/Investigations General Staff Section may be needed when
3 highly specialized information requiring technical analysis is both critical and time-sensitive to
4 life safety operations (e.g., chemical, biological, radiological, nuclear, or explosive incidents) or
5 when classified intelligence needs to be analyzed and disseminated.
6

7 Regardless of incident size, the options for placement of the Function are designed to be both
8 modular and scalable to meet incident needs. Some factors that are essential to consider in
9 determining the placement of the Function include: need for a common operating picture,
10 limiting the span of control, encouraging unity of command, and the sharing of information. The
11 14 management characteristics,³ upon which ICS is based, are factors the IC/UC should consider
12 when deciding where to place the Intelligence/Investigations Function.
13

14 The flexibility of ICS allows the Intelligence/Investigations Function to be embedded in several
15 different places within the organizational structure:
16

- 17 ○ *Within the Command Staff:*
 - 18 ● This option may be appropriate for incidents with little need for tactical information
19 or classified intelligence and where supporting Agency Representatives are providing
20 real-time information to the Command Element.
- 21 ○ *Within the Planning Section:*
 - 22 ● This is the traditional placement for this Function and is appropriate for incidents
23 with little or no investigative information requirements, nor a significant amount of
24 specialized information.
- 25 ○ *Within the Operations Section:*
 - 26 ● This option may be appropriate for incidents that require a high degree of linkage and
27 coordination between the intelligence and investigations information and the
28 operational tactics that are being employed.
- 29 ○ *As a Separate General Staff Section:*
 - 30 ● This option may be appropriate when there is a significant intelligence/investigations
31 component to the incident for criminal or epidemiological purposes or when multiple
32 investigative agencies are involved. A separate Intelligence/Investigations Section
33 may be needed when information requiring technical analysis is both critical and time
34 sensitive to life saving operations (e.g., chemical, biological, radiological, nuclear, or
35 explosive incidents) and/or when there is a need for classified intelligence.
36

37 To provide context for potential placement of the Intelligence/Investigations Function within the
38 command structure, a set of vignettes (that vary in both scope and complexity) are set forth
39 below. These illustrations provide a means of representing the different placements of the
40 Intelligence/Investigations Function. These vignettes are used *for illustrative purposes only* and

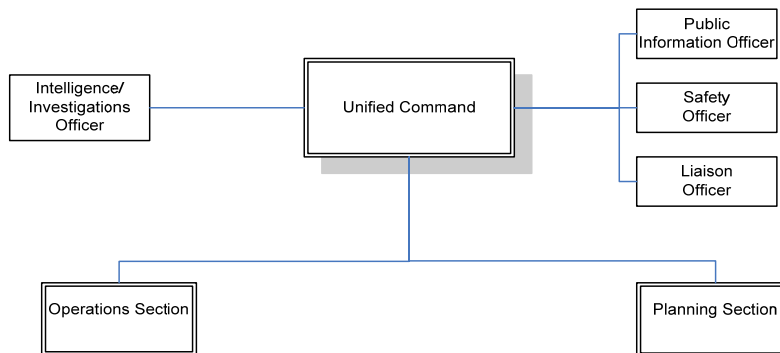
³ (1) Common Terminology, (2) Modular Organization, (3) Management by Objectives, (4) Incident Action Planning, (5) Manageable Span of Control, (6) Incident Facilities and Locations, (7) Comprehensive Resource Management, (8) Integrated Communications, (9) Establishment and Transfer of Command, (10) Chain of Command and Unity of Command, (11) Unified Command, (12) Accountability, (13) Dispatch/Deployment, and (14) Information/Intelligence Management.

1 the different placements of the Function are but one example of a path an IC/UC may choose to
2 follow during an incident. The following vignettes will identify aspects of particular incidents or
3 planned events that will assist the IC/UC in determining where to locate the
4 Intelligence/Investigations Function. As noted above, the management characteristics of ICS and
5 the principles of NIMS are the primary factors the IC/UC should consider when determining the
6 placement of the Function. Other placement decisions could be made based on incident needs,
7 resources, personnel, constraints, etc.⁴ In some incidents (or in some jurisdictions) the IC/UC
8 may automatically create a General Staff Section for the Intelligence/Investigations Function at
9 the outset of an incident.

11 **Vignette 1—As Part of the Command Staff**

13 For over 12 hours a fire (cause unknown) has been burning at used tire warehouse. Several flair-
14 ups in the smoldering tire pile continue to occur requiring constant attention of response
15 personnel. Several local response agencies are on-scene including fire, police, HazMat, and
16 environmental protection. Since this is the second fire to occur at this location in recent months,
17 there have been inquiries into the business' ownership and operations. The UC, based on
18 information received, determines that there is a need for an Intelligence/Investigations Officer to
19 act in an advisory capacity regarding the results of the investigation into the tire company. The
20 figure below shows an example of this organizational structure.

21
22 **Figure 1: Intelligence/Investigations in the Command Staff**



24
25 Unlike the Law Enforcement Branch (within the Operations Section), whose primary duties is to
26 setup and control the perimeter, protect the public and responders, etc., the
27 Intelligence/Investigations Officer within the Command Staff provides direct input to the IC/UC
28 and recommendations for any information being received about the nature or cause of the event.
29 The information given to the IC/UC will not compromise sources or sensitive data, but will only
30 consist of information or action points necessary to inform incident management decisions.

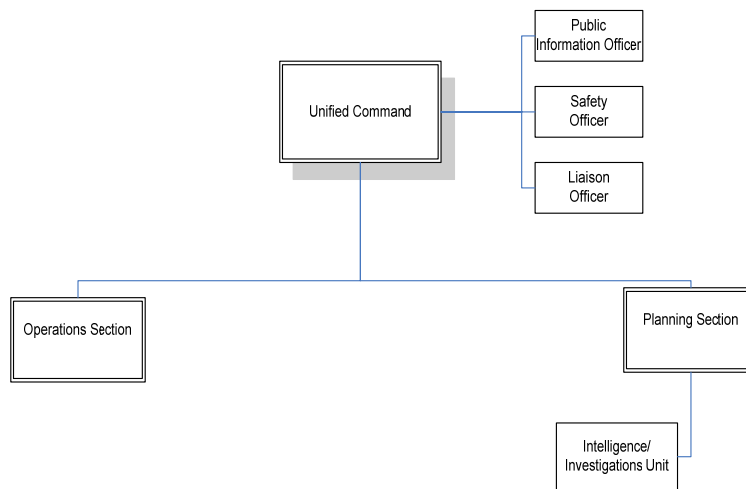
31
⁴ In an actual incident, organizations outside those identified in these vignettes (from all levels of government, the private sector or nongovernmental organizations) may be incorporated into the response efforts.

1 The Intelligence/Investigations Officer also provides technical knowledge and input during
2 planning meetings. Utilizing an Intelligence/Investigations subject matter expert as part of the
3 Command Staff at the beginning of an incident may allow for more efficient integration of
4 additional intelligence/investigations personnel.

5
6 **Vignette 2—As a Unit within the Planning Section**

7
8 Division I college football is extremely popular and draws hundreds of thousands of visitors to
9 stadiums around the country. With such large crowds in confined locations, the potential for an
10 incident is a constant concern to authorities. During the months preceding the start of the season,
11 Incident Management Teams (IMTs) are assembled using a Unified Command Structure. The
12 Planning Section personnel (representing the university, the town, first responders, etc.) lead the
13 team to develop their strategy for gathering intelligence prior to game day and responding to an
14 incident should one occur. As a result of the frequency of the games (weekly), a large amount of
15 intelligence is being gathered and reported, thereby requiring more personnel and assistance than
16 an individual Intelligence/Investigations Officer can provide; therefore, the Function may be
17 located as a Unit within the Planning Section. The figure below shows an example of this
18 organizational structure.

19
20 Figure 2: Intelligence/Investigations as part of Planning



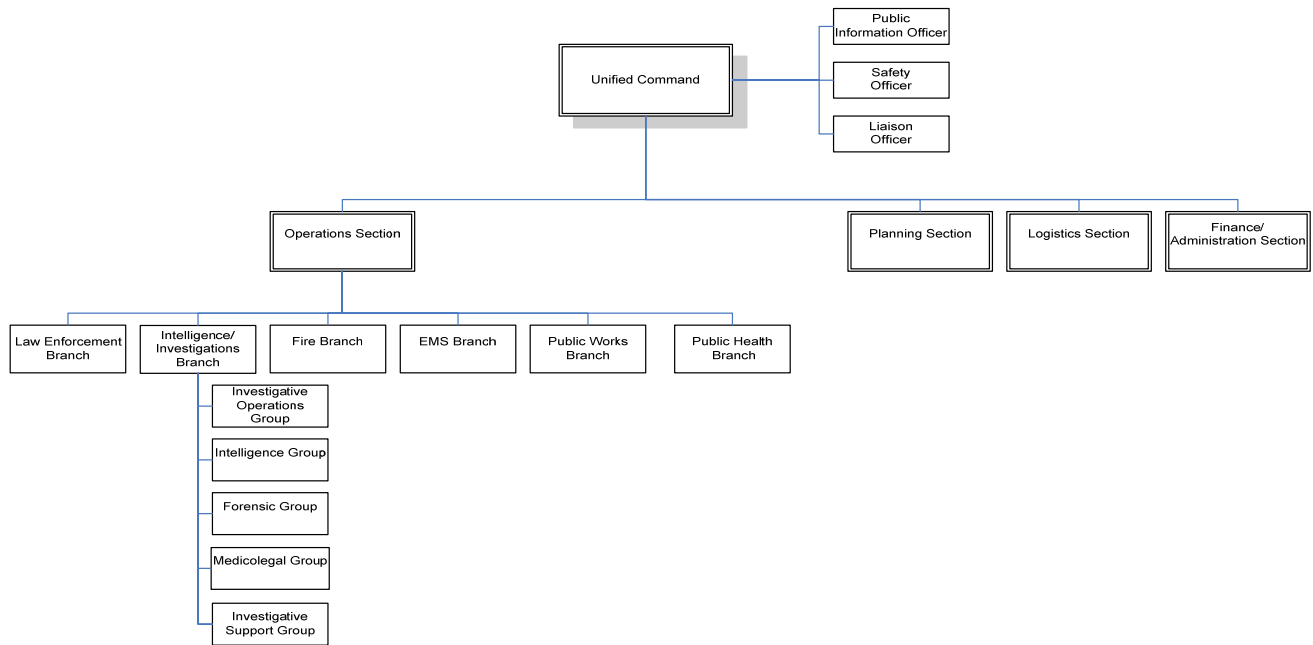
22
23
24 The nature of an Intelligence/Investigations Unit within the Planning Section will vary
25 depending on the circumstances surrounding each incident or planned event. Certain incidents
26 may necessitate the formation of two or more intelligence/investigations units; working within
27 the ICS framework, these units should be coordinated to ensure their planning activities do not
28 conflict.

29
30 **Vignette 3—As a Branch within the Operations Section**

31
32 An annual gathering of a controversial organization has sparked protests in the neighborhood
33 surrounding the planned event. A small Incident Command structure quickly expands as

1 additional resources are called to the scene. Civil unrest is breaking out, resulting in numerous
2 fires, acts of vandalism, and damage to utilities. Many fights begin as organizational factions and
3 protesters clash. Suddenly, gunfire erupts within the crowd. Two people are killed and several
4 others are injured. The crowd begins to disperse but several large pockets remain in place
5 making the numerous operational tasks difficult. The IC elects to establish the Function as a
6 Branch within the Operations Section as additional investigators are being called in to assist with
7 interviewing witnesses, tracking down leads, and processing evidence. Groups may be created
8 within the Branch to further delineate these specific intelligence/investigations responsibilities.
9

10 Figure 3: Intelligence/Investigations as Part of Operations
11



12
13
14 **Vignettes 4 & 5 —As a Section**

15 The following are two vignettes illustrating the placement of the Intelligence/Investigations
16 Function as a General Staff Section.

17
18 **Vignette 4**

19
20 Dozens of people in several contiguous jurisdictions have presented to hospitals and other health
21 care facilities within the past four days complaining of gastro-intestinal distress. Many of those
22 affected are calling 911 dispatch centers to request treatment. This larger than normal number of
23 911 calls is putting a strain on local first responders. Hospitals are treating these individuals for
24 potential food poisoning and due to the rapid rise in the rate of occurrence; hospitals and other
25 care providers have been reporting the cases to the public health authorities. Medical
26 professionals believe that the cases are related but are unable to determine the common linkage.
27 Public Health investigators are working to uncover potential commonalities. A Unified
28 Commander structure is established to manage the incident. Due to the large volume of

1 intelligence/investigations activities, the UC determines that the Intelligence/Investigations
2 Function should be a General Staff Section. A Section Chief drawn from the public health arena
3 has been selected to lead the function. This will allow the Operations Function to concentrate on
4 pre-hospital and health care facility activities. Figure 4 below shows an example of this
5 organizational structure.
6

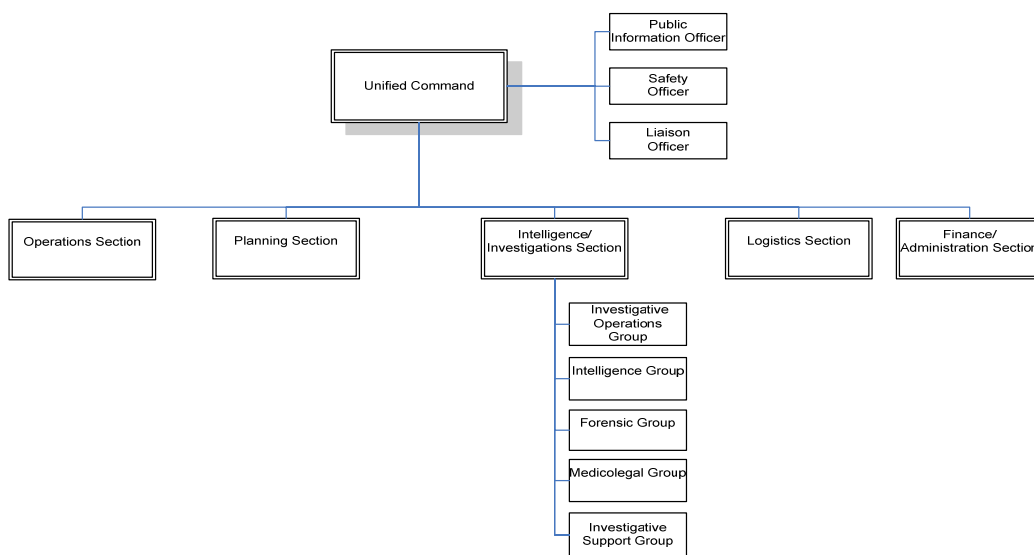
7 **Vignette 5**

8
9 A freight train hauling volatile hazardous materials leaves a downtown station. There is a loud
10 sound and the train derails causing a hazardous material to spill into a small river which runs
11 parallel to the railroad tracks and an interstate highway. The initial response to the incident
12 involves local law enforcement, fire departments, and emergency medical services.
13 Environmental and public health investigators have responded and are testing water in the nearby
14 river, as well as, monitoring the air for pollutants. The interstate highway is closed for 2 miles in
15 both directions, and the adjacent town is being evacuated. Unified Command is established.
16

17 The train conductor and other railway workers are rescued from the train wreckage. The
18 conductor states that there was nothing wrong with the train when he did his pre-departure
19 checks, and a railroad company engineer reports that the tracks were recently inspected and no
20 defects were detected. A witness states he saw a suspicious person near the tracks several
21 minutes before the derailment and observed what appeared to be a small explosion.
22

23 The UC elects to establish the Intelligence/Investigations Function as a General Staff Section to
24 allow for more intelligence/investigations personnel and resources to be assigned to the incident.
25 This placement will also ensure the smooth integration of local, State and Federal law
26 enforcement investigators, the National Transportation Safety Board and other subject matter
27 experts.
28

29 Figure 4: Intelligence/Investigations as a General Staff Section
30



31
32

1 Establishing an Intelligence/Investigations Section is based on the determination that the nature
2 of the incident requires a large investigation and/or a large amount of information to be collected,
3 analyzed, controlled and disseminated. Regardless of the circumstances, it is imperative that
4 regular and timely updates from the Intelligence/Investigations Section are provided to the
5 IC/UC, as incident management decisions may be based on those updates.

6 **Maintaining Linkages between Intelligence/Investigations Section and** 7 **Incident Command Structure**

8
9 In cases where the Intelligence/Investigations Function is organized as a General Staff Section,
10 an appropriate Section management organization should be established. While the
11 organizational relationships within ICS will remain, the nature of some incidents may constrain
12 the type and scope of information that may be shared. For example:

- 13
14 ○ *Link to the Command Staff:* Information and intelligence must be provided to the
15 Command Staff in a timely, accurate and accessible form (sensitive or classified
16 information may need to be put into an accessible form if recipients do not have
17 appropriate clearances). Depending upon the scope, complexity, significance and
18 duration of the Intelligence/Investigations Function, an Intelligence/Investigations
19 Section Technical Specialist may be assigned to the Incident Command Post to ensure
20 seamless communication and coordination. This may be particularly important when the
21 incident involves a significant threat of potential unlawful activity including terrorism or
22 intelligence/investigations activities involve a substantial amount of Classified National
23 Security information.
- 24
25 ○ *Link to the Planning Section:* Tactical information and reports should be given to the
26 Planning Section, so Incident Action Plans can be updated for the next planning period.
27 As the Intelligence/Investigations Section receives information and intelligence from
28 varying sources, it should work closely with the Planning Section to assist in processing
29 information for planning purposes.
- 30
31 ○ *Link to the Operations Section:* A high degree of coordination is necessary between the
32 Intelligence/Investigations Section and the Operations Section as a significant portion of
33 intelligence/investigations personnel have duties that place them on-scene and operating
34 in tandem with many other emergency management and response personnel. The
35 intelligence/investigations information obtained may greatly affect the operational tactics
36 that are being employed. Whenever possible, constant coordination will be required to
37 ensure that operational objectives do not conflict with evidence recovery operations;
38 however life safety issues will take priority over investigative operations if the safety of
39 the public or responders is in jeopardy.

40
41 An Operations Section Technical Specialist may be assigned to the
42 Intelligence/Investigations Section Work Area; likewise, an Intelligence/Investigations
43 Section Technical Specialist will be assigned to the Operations Section Work Area.
44 Depending upon the scope, complexity, significance and duration of the activities
45 required, the technical specialists may act in a supervisory capacity.

1 **Organizational Connectivity and Deconfliction**⁵

2
3 Situational awareness will be enhanced to support preparedness efforts through the sharing of
4 pre-incident information, intelligence and real-time incident updates. The aim of all entities
5 involved in processing and sharing information should be the development of a common
6 operating picture – day-to-day and during an incident or planned event.

7
8 Improving information sharing in the post–September 11 world requires
9 an environment that supports the sharing of information across all levels
10 of government, disciplines, and security domains... Information
11 acquired for one purpose, or under one set of authorities, might provide
12 unique insights when combined, in accordance with applicable law, with
13 unrelated information from other sources, and therefore we must foster a
14 culture of awareness in which people at all levels of government remain
15 cognizant of the functions and needs of others and use knowledge and
16 information from all sources to support counterterrorism efforts.⁶

17
18 Sources of this information may include many of the following:

- 19
20 ○ Existing intelligence/investigative activities and organizations may have information,
21 leads and resources. Joint Terrorism Task Forces, local or regional fusion centers,
22 regional intelligence sharing projects (RISS consortiums),⁷ and adjacent local, Tribal or
23 State organizations should be linked to any incident-specific activity.
- 24 ○ Situational clearinghouses such as the National Severe Storm Center/National Oceanic
25 and Atmospheric Administration, the National Interagency Fire Center, Centers for
26 Disease Control, etc.
- 27 ○ Dispatch call centers, and local and departmental EOCs/DOCs may have relevant
28 information.
- 29 ○ Mutual aid, Emergency Management Assistance Compact, Emergency Federal
30 Assistance to Law Enforcement (Allocation of Funds and Other Assistance)⁸ or similar
31 arrangements.
- 32 ○ In an incident involving primary Federal investigative jurisdiction, the FBI will likely
33 stand up a JOC and Joint Interagency Intelligence Support Element.
- 34 ○ Family Assistance Centers may have information about the local population that they
35 serve during an incident.
- 36

⁵ Deconfliction is the avoidance of duplication or interference.

⁶ See: http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf

⁷ The RISS Program is composed of six regional projects that share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Although the six RISS projects are primarily drug-crime focused, they may select additional target crimes, and provide a range of services to assist their member agencies. Mandatory services include information sharing through a criminal intelligence data base; provision of analytical services; and provision of telecommunication services to facilitate the flow of information between the project and its members.

⁸ 28 CFR §65.12: “In accordance with the purposes and limitations of this subdivision, members of the Federal law enforcement community may provide needed assistance in the form of equipment, training, intelligence information, and personnel. The application may include requests for assistance of this nature.”

1 Use and Organization of Groups

2
3 In situations where the span of control exceeds recommended ratios (1: 3-7), the
4 Intelligence/Investigations Section may be divided into Groups representing specific mission
5 areas. When applicable, the Intelligence/Investigations Section Chief may create one or more
6 Groups within the Section and designate a Group Supervisor for each Group. The Section Chief
7 must notify the Planning Section and, when applicable, Incident Command, regarding the
8 number of personnel assigned to the Section and to each Group. If any of the Groups are not
9 utilized (or have been deactivated), the Section Chief will be responsible for the management of
10 those responsibilities.

11
12 The flexibility within ICS allows for some variation in Group names which may be designed to
13 meet the needs of the incident. Though the responsibilities of the Groups may not be altered, the
14 delineated tasks within each Group may be modified depending on incident needs.

15
16 Groups will be utilized based on the needs of the incident. Examples of Groups that may be
17 activated include the following:

- 18
19 • *Investigative Operations Group*: responsible for the overall investigative effort. The
20 Group Supervisor may designate individuals to complete the following tasks:
 - 21 ○ Tracking and managing personnel assignments
 - 22 ○ Keeping a record of chronological events
 - 23 ○ Managing evidence
 - 24 ○ Coordinating tactical operations
 - 25 ○ Managing and coordinating physical surveillance
 - 26 ○ Managing and coordinating electronic surveillance
 - 27 ○ Tracking telephone and computer records
- 28
29 • *Intelligence Group*: responsible for obtaining unclassified, classified, and open source
30 intelligence. The Group Supervisor may designate individuals to complete the following
31 tasks:
 - 32 ○ Addressing requests for information
 - 33 ○ Coordinating intelligence requirements
 - 34 ○ Coordinating and tracking the collection of intelligence
 - 35 ○ Producing and analyzing intelligence
 - 36 ○ Coordinating the dissemination of information
 - 37 ○ Coordinating the protection of national infrastructure
 - 38 ○ Acting as the Security Officer for Classified National Security information
- 39
40 • *Forensic Group*: responsible for ensuring the integrity of the crime scene and forensic
41 evidence. The Group Supervisor may designate individuals to complete the following
42 tasks:
 - 43 ○ Coordinating aspects relevant to the crime scene
 - 44 ○ Coordinating CBRNE/HazMat issues
 - 45 ○ Coordinating bomb operations
 - 46 ○ Managing the analysis of forensic evidence

- 1 ○ Managing the analysis of digital and multi-media evidence
- 2
- 3 • *Medicolegal Group*: responsible for ensuring that missing and unidentified persons, and
- 4 decedents are expeditiously investigated and identified and that required notifications are
- 5 made in a timely manner. This includes the collection of ante-mortem information and
- 6 exemplars in a Family Assistance Center. Additionally, the Medicolegal Group is
- 7 responsible for coordinating a medicolegal investigation conducted by a medicolegal
- 8 death investigator. The Group Supervisor may designate individuals to complete the
- 9 following tasks:
 - 10 ○ Reporting, tracking, investigating, and resolving missing and unidentified Persons
 - 11 ○ Conducting Fatality Management investigative activities
 - 12 ○ Establishing ante-mortem and missing persons data collection within a Family
 - 13 Assistance Center
- 14
- 15 • *Investigative Support Group*: responsible for ensuring that required investigative
- 16 personnel are made available and necessary resources are distributed, maintained,
- 17 safeguarded, stored and returned. The Group Supervisor will coordinate with Operations
- 18 or Logistics Section Chiefs to assist in:
 - 19 ○ Activating an appropriate number of intelligence/investigations worksites and
 - 20 situating each of the worksites at an appropriate location
 - 21 ○ Determining the need to designate a Staging Area Manager for Intelligence/
 - 22 Investigations Section activities
 - 23 ○ Subject to available personnel resources, the Group Supervisor may wish to
 - 24 appoint a subordinate to complete the following tasks:
 - 25 • Manage the worksite
 - 26 • Coordinate resources
 - 27 • Facilitate and coordinate communications
 - 28 • Coordinate site and personnel security

29 **Use and Organization of Branches**

30

31 In specific instances when the Intelligence/Investigations Section must be performed by an

32 extremely large number of personnel and span of control problems must be prevented or resolved

33 (i.e., too large to support the direct reporting of Groups to the Section Chief), or when other

34 appropriate circumstances exist, then the Intelligence/Investigations Section Chief may activate

35 one or more Branches within the Intelligence/Investigations Section instead of one or more

36 Groups, and designate a Branch Director for each activated Branch.

- 37 • Investigative Operations Branch
- 38 • Intelligence Branch
- 39 • Forensic Branch
- 40 • Medicolegal Branch
- 41 • Investigative Support Branch
- 42

1 **Summary**

2
3
4
5
6
7
8
9

As explained above, the Intelligence/Investigations Function within ICS provides a flexible and scalable framework that will allow for the integration of intelligence/investigations information. This document provides guidance on how to utilize and integrate this Function within ICS, while adhering to the concepts and principles of NIMS. It also provides information intended for the ICS practitioner to assist in the decision-making process regarding the placement of the Function within the command structure.

INTELLIGENCE/INVESTIGATIONS FUNCTION FIELD OPERATIONS GUIDE

Purpose and Organization

This Intelligence/Investigations Function Field Operating Guide (IIFOG) is designed to assist those implementing the Intelligence/Investigations Function within an Incident Command structure during incidents or planned events, regardless of type, size, location or complexity. This document will describe the Function as a General Staff Section in order to illustrate the universe of potential tasks and responsibilities within the Function. There are several other options for placing this Function within the Incident Command structure,⁹ and this guide can act as a tool to provide instruction and principles for those alternate locations.

The IIFOG is not a policy document and does not replace Emergency Operations Plans (EOPs), laws, regulations and ordinances. Rather, it is intended to provide guidance for personnel assigned to an incident or planned event. The information contained in this document is intended to supplement the user's experience, training and knowledge in the performance of intelligence/investigations activities relative to the identified circumstances and provide a model for organizing the process and management of intelligence/investigations operations and activities.

The first portion of the IIFOG provides an overview of the Function as a whole and discusses aspects (setup, planning, logistics/communications, resource management and coordination) that apply to the General Staff Section level of the Function. The second portion of the IIFOG provides more information on the Groups and relevant task areas that can be set up under the Intelligence/Investigations Section. Finally, the IIFOG includes an acronym list and definitions to highlight terminology applicable to the Function. In brief, the document contains the following:

- Intelligence/Investigations Functional Overview
 - Initial Setup
 - Use of Deputies
 - Internal/External Activities and Relationships (including planning, logistics, and resource management)
- Physical Location and Work Area
- Groups and Structure within the Section (including a description of each of the five potential Groups)
- Acronym List
- Definitions

⁹ Potential placements include: Within the Command Staff, the Planning Section, the Operations Section or as a General Staff Section.

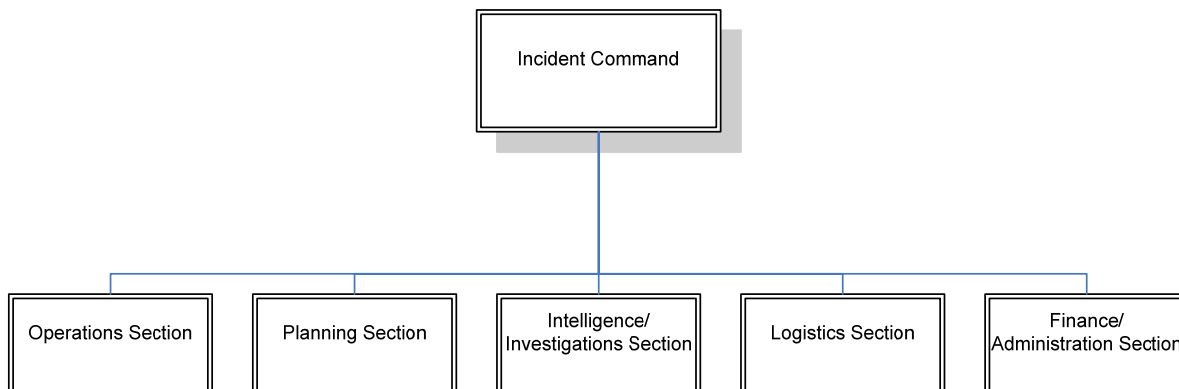
1 Personnel using the IIFOG should have a detailed understanding of NIMS and ICS to ensure that
2 they can effectively set up and operate an Intelligence/Investigations Function. *The contents of*
3 *this document are not intended to serve as a substitute for formal required training and good*
4 *judgment.* All agencies and jurisdictions should ensure that responders receive adequate and
5 appropriate training to perform their assigned duties and tasks within the Function.
6

7 The IIFOG is designed so that users may tailor the following pieces based on their specific
8 needs. As a new ICS concept, the Intelligence/Investigations Function is still under
9 development. For this reason, the guidance provided in the IIFOG is not as comprehensive as
10 that contained in the Emergency Responder FOG (ERFOG). In the future, more specific job aids
11 will be created and the guidance in the IIFOG further developed. Local emergency managers
12 may also wish to create customized guides containing local information and checklists.
13

14 Intelligence/Investigations Functional Overview

15
16 This document is intended to describe the Intelligence/Investigations Function when it is
17 implemented as a General Staff Section equivalent to other Sections such as Planning and
18 Operations. The following portion of the IIFOG addresses considerations relevant to the Section
19 as a whole (or to the Section Chief or Deputy Section Chief). Topics covered include steps and
20 considerations for the initial setup of the Section, the use of deputies, and internal and external
21 relationships in four areas: planning, logistics/communications, resource management, and
22 coordination, as shown in the figure below.
23

24 Figure 5: Intelligence/Investigations as a General Staff Section
25



26 **Initial Setup**

27
28 The following is a list of suggested tasks and actions that the Incident Commander/Unified
29 Command (IC/UC) and/or the potential Intelligence/Investigations Section Chief may want to
30 consider when initially establishing the Intelligence/Investigations Function. This list may be
31 tailored to the jurisdiction and/or incident, as appropriate.
32

- 33 ○ Collect and evaluate all available information while responding to the incident scene.
- 34 ○ Obtain a comprehensive briefing regarding the incident.

- 1 ○ Confer with the IC/UC regarding how the Intelligence/Investigations Function should
2 be established and organized.¹⁰
- 3 ○ Assume control regarding the Intelligence/Investigations Section, and ensure all
4 appropriate incident personnel are promptly notified.
- 5 ○ When necessary, ensure relevant information regarding Intelligence/Investigations
6 activities has been implemented and is communicated to the appropriate personnel
7 and the communications dispatcher.
- 8 ○ Confer with the IC/UC to determine those intelligence/investigations agencies that
9 will be involved in the incident.
- 10 ○ Confer with the Operations Section, Logistics Section and Safety Officer regarding
11 force protection, security, health and safety issues.
- 12 ○ Establish the Intelligence/Investigations Section work area at a secure location a
13 reasonable distance from the Operations Section work area and the Incident
14 Command Post (ICP).
- 15 ○ Ensure required audio, data, image and text communications equipment is obtained,
16 and communication procedures are implemented.
- 17 ○ Ensure a specific verbal or, if applicable, written Intelligence/Investigations Section
18 communications plan is prepared and provided to the Logistics Section.
- 19 ○ Notify an investigator, identify a point of contact, frequently communicate and
20 coordinate with off-incident facilities (e.g., hospital, business, residence, Intelligence
21 Fusion Center, FBI JOC, Family Assistance Center) involved regarding the
22 investigation of the incident and any other facilities or sites associated with
23 intelligence/investigations activities.
- 24 ○ Assign an Intelligence/Investigations Section Technical Specialist to the ICP.
- 25 ○ Ensure an Operations Section Technical Specialist is assigned to the
26 Intelligence/Investigations Section work area.
- 27 ○ Ensure an Intelligence/Investigations Section Technical Specialist is assigned to the
28 Operations Section work area.
- 29 ○ Designate one or more Deputy Intelligence/Investigations Section Chiefs.
- 30 ○ Activate one or more Groups or Branches.
- 31 ○ Ensure resources that respond directly to the incident scene (both initially and in later
32 deployments) are:
 - 33 a. Immediately identified.
 - 34 b. Checked-in.
 - 35 c. Properly equipped.
 - 36 d. Wearing the required personal protective equipment, if appropriate.
 - 37 e. Appropriately organized.
 - 38 f. Directed to continue performing the current assignments or assigned to an initial
39 assignment, and/or (if already on-scene) reassigned and deployed to appropriate
40 new assignments or, when necessary, directed to respond to one or more
41 designated Staging Areas or off-incident locations.
- 42 ○ Request the necessary and appropriate operational and support resources, and ensure
43 there is a controlled response of the requested resources.

¹⁰ From this point forward, Intelligence/Investigations will be referred to as a General Staff Section. Prior to this point, the term “function” is used to describe Intelligence/Investigations in any of its four potential locations in the ICS command structure.

- 1 ○ Ensure that an appropriate number of Intelligence/Investigations Section Staging
- 2 Areas are activated and a Staging Area Manager is designated for each Staging Area.
- 3 ○ Ensure intelligence/investigations related Incident Objectives, strategies and priorities
- 4 are formulated and documented.
- 5 ○ Ensure a comprehensive investigative plan is formulated and documented.
- 6

7 ***Use of Deputies***

8 While the previous section illuminated many overall responsibilities that would fall under the
9 Intelligence/Investigations Section Chief, depending on the size and scope of the incident, a
10 Deputy Section Chief (or Chiefs) may be appointed by the Section Chief. The following should
11 be taken into consideration in the selection of this individual, in addition to some responsibilities
12 that he or she might have as Deputy Intelligence/Investigations Section Chief. It is important to
13 remember that the use of Deputies is optional, according to the needs of the incident, as
14 determined by the Section Chief.

15 *Qualifications*

16 The Deputy Intelligence/Investigations Section Chief:

- 17 ○ Should have the same qualifications and experience as the Intelligence/Investigations
- 18 Section Chief.
- 19 ○ Must be capable of assuming the Intelligence/Investigations Section Chief position in
- 20 full or temporarily when the Section Chief is absent.
- 21
- 22

23 *Responsibilities*

24 The role of the Deputy Intelligence/Investigations Section Chief is flexible, and the Deputy
25 Intelligence/Investigations Section Chief may:

- 26 ○ Collect and analyze incident related information and data.
- 27 ○ Monitor and evaluate the current situation and estimate the potential future situation.
- 28 ○ Monitor and assess the effectiveness of the Intelligence/Investigations Section
- 29 organizational structure.
- 30 ○ Monitor and evaluate the intelligence/investigations related resources, support and
- 31 reserves.
- 32 ○ Monitor and assess the performance of the Intelligence/Investigations Section
- 33 personnel.
- 34 ○ Monitor and evaluate the implementation and effectiveness of the investigative plan
- 35 and the intelligence/investigations aspects of the Incident Action Plan (IAP).
- 36 ○ Monitor and evaluate intelligence/investigations related activities.
- 37 ○ Identify, evaluate and resolve intelligence/investigations related requirements and
- 38 problems.
- 39 ○ Function as the “eyes and ears” of the Intelligence/Investigations Section Chief.
- 40 ○ Make important notifications (e.g., Emergency Operations Center, Regional
- 41 Intelligence Fusion Center, FBI JOC, Communications Dispatcher, Family Assistance
- 42 Center)
- 43 ○ Participate in Planning Section meetings, when appropriate.
- 44

45 *Origin of Deputies*

1 One or more of the Deputy Intelligence/Investigations Section Chiefs may be members of a
2 different agency than the Intelligence/Investigations Section Chief. Their member agency may
3 be one that has:

- 4 ○ Legal jurisdiction or geographic responsibility of the incident scene.
- 5 ○ Legal jurisdiction or geographic responsibility regarding the
6 intelligence/investigations aspects of the incident.
- 7 ○ Significant resources involved in the incident.
- 8 ○ Been significantly affected by the incident.

10 ***Internal/External Intelligence/Investigations Activities and*** 11 ***Relationships***

12 Coordination is essential for effective and efficient management of any incident or planned
13 event. When specialized resources, such as investigators, become engaged in activities during an
14 incident, the need for coordination increases as other operational activities may conflict with
15 intelligence/investigations activities.

16
17 The information contained below describes three aspects (planning, logistics and resource
18 management) of how the Intelligence/Investigations Section will perform as a whole. It
19 discusses the internal and external activities of each aspect in order to define the actions within
20 the Section as well as how they relate to other Sections within the command structure.

21
22 In addition to the coordination requirements within the three aspects, there are several other steps
23 an Intelligence/Investigations Section Chief may take to ensure adequate communication both
24 inside and outside the Intelligence/Investigations Section. The Section Chief may:

- 25 ○ Schedule and conduct regular meetings and briefings with all of the
26 Intelligence/Investigations Deputy Section Chiefs, Group Supervisors, Managers and
27 Coordinators to review current intelligence/investigations status and progress.
- 28 ○ Schedule and conduct periodic meetings with all of the Intelligence/Investigations personnel.
- 29 ○ Establish and maintain liaison and integrated operations with all levels and functions within
30 the incident management organization while adhering to the established chain of command
31 and ICS protocols.
- 32 ○ Until all relevant intelligence/investigations activities have been completed, confer with the
33 Command and General Staff to ensure procedures are implemented to:
 - 34 ○ prevent interference with intelligence/investigations activities
 - 35 ○ avoid disturbance of known or suspected crime scenes or investigative scenes
 - 36 ○ avoid disturbance of decedents
- 37 ○ Frequently communicate and coordinate with the Operations Section regarding tactical
38 intelligence/investigations related activities (e.g., warrant executions, arrests, searches,
39 seizures, physical surveillance, electronic surveillance, covert entries, stops/detentions,
40 directed enforcement operations, undercover officer operations, identification activities and
41 epidemiological surveillance).
- 42 ○ Confer with the Command and General Staff to ensure all Intelligence/Investigations Section
43 activity is continually coordinated with the appropriate governmental agencies,
44 nongovernmental organizations and the private sector. This includes the US Intelligence
45

- 1 Community, and the law enforcement, homeland security, military and international
2 security/liaison communities.
- 3 ○ Ensure the Public Information Officer:
 - 4 ○ Provides assistance regarding public affairs and media related activities.
 - 5 ○ Monitors information disseminated by the media, governmental agencies,
6 nongovernmental organizations and the private sector, and immediately forwards
7 any relevant information to the Intelligence/Investigations Section.
 - 8 ○ Coordinate with the Public Information Officer to ensure public information related activities
9 do not violate or contravene operations security, operational security or information security
10 procedures.

11
12 Planning

13 Coordinated planning is a keystone of both NIMS and more specifically, ICS. How
14 Sections plan together can play a large role in determining the degree of success in
15 response operations, including those related to intelligence/investigations activities. In
16 particular, staff responsible for Intelligence/Investigations Section planning should make
17 certain that the intelligence/investigations related incident objectives do not conflict with
18 overall incident strategies and objectives. In those instances where a conflict may arise, it
19 is necessary to deconflict those issues prior to engaging in actions that could compromise
20 the incident objectives or endanger personnel. Below are some tasks and responsibilities
21 relating to both the internal and external planning efforts of the Intelligence/Investigations
22 Section. It is important to keep in mind that many of these activities can have both
23 inward and outward-facing aspects.

24
25 Internal Tasks/Responsibilities:

- 26 ○ Analyze incident or planned event-related information and data, evaluate the
27 current situation, and estimate the potential future situation.
- 28 ○ Ensure required resources, reserves, and support are identified and requested in
29 the appropriate manner.
- 30 ○ Ensure problems, requirements, issues and concerns are identified and resolved.
- 31 ○ Ensure intelligence/investigations incident objectives and strategies are
32 formulated and documented.
- 33 ○ Ensure all of the intelligence/investigations aspects and components of the IAP
34 and the Demobilization Plan are implemented.

35
36 External Tasks/Responsibilities:

- 37 ○ Confer with the Planning Section regarding planning functions and activities.
- 38 ○ When appropriate, participate in Planning Section meetings.
- 39 ○ Assist in setting the overall incident priorities to ensure that
40 Intelligence/Investigations Section priorities are addressed.
- 41 ○ Assist in the formulation and preparation of the IAP and provide
42 intelligence/investigations:
 - 43 ■ Organization chart
 - 44 ■ Supporting plan
 - 45 ■ Supporting materials/attachments (e.g., maps, data, images, matrices,
46 briefings, situation reports, assessments)

- 1 ○ Confer with the Planning Section regarding the intelligence/investigations
2 aspects and components of the IAP including:
 - 3 ▪ Incident objectives, strategies and priorities
 - 4 ▪ Information on resources, reserves and support
 - 5 ▪ Operations
 - 6 ▪ Activities
- 7 ○ Ensure intelligence/investigations needs are considered when the incident
8 objectives and strategies are formulated and the IAP is developed.
- 9 ○ Confer with the Planning Section regarding the intelligence/investigations
10 aspects and components of the Demobilization Plan.
- 11 ○ Ensure activities related to the formulation, documentation and dissemination of
12 the IAP and other planning activities do not violate operations security,
13 operational security or information security procedures, measures and activities.
- 14 ○ Confer with the Planning Section regarding documentation and records
15 management procedures, measures and activities.

16
17 Logistics/Communications

18 Incidents that warrant the establishment of an Intelligence/Investigations Section will
19 often require provisions for secure or other special communications capabilities. Below
20 are some tasks and responsibilities relating to both the internal and external
21 logistics/communications efforts of the Intelligence/Investigations Section.

22
23 Internal Tasks/Responsibilities:

- 24 ○ Ensure audio, data, image and text communications procedures, measures and
25 activities are implemented.
- 26 ○ Ensure an incident specific communications plan is prepared and implemented,
27 particularly if secure communications systems or security protocols must be
28 utilized (including communications mechanisms used to convey critical
29 information).
- 30 ○ When necessary, designate Intelligence/Investigations Section primary and
31 secondary system radio channels and primary and secondary point-to-point radio
32 channels.
- 33 ○ When necessary, ensure that a sufficient number of secure communications
34 devices are obtained [e.g., Secure Telephone Unit (STU III), Secure Telephone
35 Equipment (STE), mobile Sensitive Compartmented Information Facility
36 (SCIF)].
- 37 ○ Ensure a verbal or written Intelligence/Investigations Section communications
38 plan is prepared.
- 39 ○ Ensure all intelligence/investigations personnel are familiar with life-safety
40 warning communications protocols used by other response organizations for
41 imminent life-threatening situations.

42
43 External Tasks/Responsibilities:

- 44 ○ Confer with the Logistics Section (Communications Unit Leader) regarding
45 communications systems, guidelines, constraints and protocols.
- 46 ○ Communicate and coordinate the Intelligence/Investigations Section

1 communications plan with the Logistics Section; and when possible, provide
2 them a copy of the written Intelligence/Investigations Section communications
3 plan.

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

8 9 Resource Management

10 Intelligence/investigations often require specialized equipment and trained personnel
11 resources which may or may not be suited for inclusion with other incident resources.
12 Specialized resources may require added security and confidentiality; as such, it is
13 necessary for the Intelligence/Investigations Section to coordinate with the Logistics
14 Section and other Command Staff to ensure adequate resource management processes are
15 in place. Below are some tasks and responsibilities relating to both the internal and
16 external resource management efforts of the Intelligence/Investigations Section.

17 18 Internal Tasks/Responsibilities:

- 19 ○ Evaluate the current situation, estimate the potential future situation, determine
20 the resource needs for one or more operational periods, and request the necessary
21 operational and support resources (e.g., personnel, equipment, and vehicles).
- 22 ○ Maintain control of requested resources and ensure that requested resources do
23 not deploy directly to the incident scene. (Follow standard ICS protocols for
24 mobilization, dispatch, deployment, check-in and task assignments.)
- 25 ○ Ensure that an appropriate number of Intelligence/Investigations Section Staging
26 Areas are activated and a Staging Area Manager is designated for each of the
27 activated Staging Areas.

28 29 External Tasks/Responsibilities:

- 30 ○ Confer with Command and General Staff to identify anticipated
31 intelligence/investigations resource needs.
- 32 ○ Ensure resources that initially responded directly to the incident scene, as well as
33 those later requested, are:
 - 34 ▪ Immediately identified.
 - 35 ▪ Checked-in (authorized for on-scene activities).
 - 36 ▪ Properly equipped.
 - 37 ▪ Wearing the appropriate personal protective equipment (PPE) for the
38 known or suspected threat or hazard.
 - 39 ▪ Organized consistent with the ICS protocols.
 - 40 ▪ Issued instructions regarding current or new assignments and deployments
41 or redeployment.

42 43 44 **Intelligence/Investigations Physical Location and Work Area**

1 The sensitive nature of intelligence/investigations operations and the need for consistent
2 communication with the other portions of the Command Structure create unique considerations
3 for the physical location of the Intelligence/Investigations Section in relation to Incident
4 Command and other General Staff Sections. The intelligence/investigations work area is the
5 location where the Intelligence/ Investigations Section Chief and appropriate staff will remain, as
6 well as manage, coordinate and direct all of the intelligence/investigations operations, functions
7 and activities. Following are some considerations to remember as the intelligence/investigations
8 work area location is being selected and maintained.

- 9
- 10 ○ Will be established at a secure location a reasonable distance from the other
11 Command and General Staff work areas; also, absent unusual circumstances, it will
12 not be situated contiguous to the Incident Command Post or Operations Section work
13 area.
- 14 ○ Choose a location that:
 - 15 ■ Is sufficiently large.
 - 16 ■ Is a reasonable and appropriate distance from the incident scene.
 - 17 ■ Will provide safety, health, security and force protection.
 - 18 ■ Will provide easy and expeditious access and egress.
 - 19 ■ Will provide adequate workspace.
 - 20 ■ Will allow for expansion.
 - 21 ■ Will permit continuous operations.
 - 22 ■ Will provide adequate utilities, wire line and wireless communication
23 services, sanitation and other essential infrastructure and services.
- 24 ○ The intelligence/investigations work area may be any type of facility or location that
25 is available and appropriate (e.g., vehicle, trailer, tent, open area, room in a building).
- 26 ○ Confer with the Operations Section, Logistics Section and Safety Officer to ensure
27 adequate safety, health, security and force protection measures are implemented in
28 the Intelligence/Investigations work area.
- 29 ○ When necessary, specifically assign personnel to thoroughly search the location
30 where the intelligence/investigations work area is situated for any force
31 protection/security hazards, health and safety hazards.
- 32 ○ When necessary, specifically assign personnel to provide force protection/security
33 regarding non-hostile unauthorized persons, persons conducting intelligence
34 collection, surveillance or reconnaissance activities/operations, hostile persons,
35 emotionally disturbed persons, etc.
- 36 ○ When necessary, ensure identification, credentialing and badging procedures,
37 measures, functions and activities are implemented.
- 38

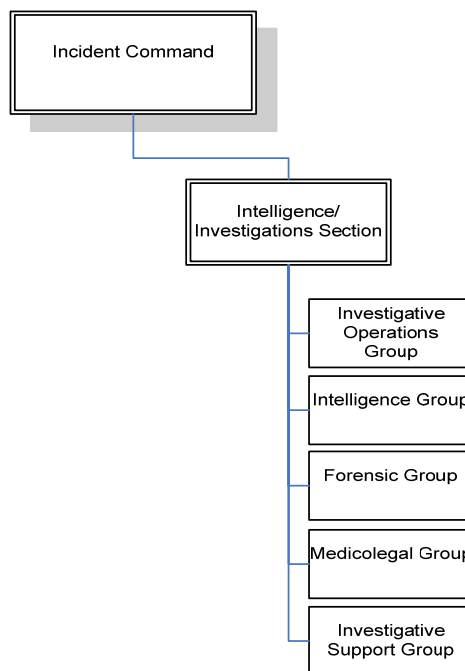
1 **Groups and Structure within the Intelligence/Investigations** 2 **Section**

3
4 When set up as a Section, the Intelligence/Investigations Section Chief has the option of creating
5 one or more Groups to oversee the activities of the Section. Suggestions for five Groups and
6 their related tasks are offered below, but it is up to the Section Chief to combine or separate
7 them, as appropriate for the particular incident or planned event, as shown in the figure below.
8

9 ***Investigative Operations Group***

10 To accomplish the mission of the Intelligence/Investigations Section, the Investigative
11 Operations Group will manage and direct the overall investigative effort and will utilize the
12 information produced by all other Groups. Generally, the primary case investigator and
13 supervisor will be assigned to the Investigative Operations Group.
14

15 Figure 6: Intelligence/Investigations Organization
16
17



18
19
20 Investigative Operations Group will ensure that:

- 21 ○ Each investigative lead/task is recorded in the assignment log or database and is
- 22 assigned to appropriate personnel in the proper priority order and sequence.
- 23 ○ Each assigned investigative lead/task is properly, completely and expeditiously
- 24 performed.

- 1 ○ Results of each assigned investigative lead/task are documented and all of the
- 2 associated materials are invoiced, safeguarded and examined.
- 3 ○ All forensic and investigative evidence (e.g., documents/text, images/photos, audios,
- 4 data) are invoiced, safeguarded and analyzed.
- 5 ○ All investigative reports and materials associated with the results of each assigned
- 6 investigative lead/task and the related forensic evidence and investigative evidence
- 7 are discussed with the appropriate personnel; and, as well as examined and evaluated
- 8 to determine whether the assigned investigative lead/task was properly performed.
- 9 ○ Each examined and evaluated investigative lead/task is categorized closed (no further
- 10 action or new leads generated) or open (additional action required).
- 11 ○ Appropriate information regarding each examined and evaluated investigative
- 12 lead/task is recorded in the assignment log or database.
- 13 ○ Results of each assigned investigative lead/task are exploited, and if applicable, one
- 14 or more subsequent additional follow-up investigative leads/tasks are identified,
- 15 recorded, assigned, performed, etc.
- 16 ○ A chronological account of the significant intelligence/investigations information,
- 17 activities, events and results are documented and if appropriate are displayed on
- 18 Situation Boards.
- 19 ○ Appropriate intelligence/investigations techniques and tactics are utilized in the
- 20 proper priority order and sequence.
- 21 ○ Required legal advice, services, documents, applications and process are obtained.
- 22 ○ Documentation and records management procedures are implemented.
- 23 ○ When appropriate, secure and obtain sources of investigatory data such as flight data
- 24 recorders, cockpit voice recorders, vehicle electronic data recorders, radar data, and
- 25 911 tapes.

26
27 The Investigative Operations Group will utilize techniques and tactics including, but not limited
28 to, the following example activities:

- 29 ○ Non-technical and technical canvasses.
- 30 ○ Interviews and interrogations.
- 31 ○ Identification procedures.
- 32 ○ Searches and seizures.
- 33 ○ Database/record queries.
- 34 ○ Electronic communication (telephone, computer) investigative records acquisition
- 35 and analysis.
- 36 ○ Physical surveillance.
- 37 ○ Electronic surveillance.
- 38 ○ Financial records acquisition and analysis.
- 39 ○ Travel records acquisition and analysis.
- 40 ○ Polygraph examinations.
- 41 ○ Undercover officer and confidential informant operations.
- 42 ○ Trash seizures and searches.
- 43 ○ Mail covers.

44
45 Depending upon the scope, complexity, and size of the Intelligence/Investigations Section, the
46 Investigative Operations Group Supervisor may activate one or more of the positions below. As

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

- 3 ○ Assignment Manager
- 4 ○ Scribe
- 5 ○ Evidence Manager
- 6 ○ Physical Surveillance Coordinator
- 7 ○ Electronic Surveillance Coordinator
- 8 ○ Electronic Communication Records Coordinator
- 9 ○ Tactical Operations Coordinator

11 ***Intelligence Group***

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

15
16 The information intake and assessment function ensures all incoming information, except the
17 results of investigative leads/tasks, is:

- 18 ○ Communicated directly to the Intelligence Group.
- 19 ○ Recorded on an Information Control form, and/or entered into an Information Control
20 database.
- 21 ○ Initially evaluated and categorized as being:
 - 22 ■ Information that may require an investigative lead/task be assigned by the
23 Investigative Operations Group. (This information will be immediately
24 communicated to the Investigative Operations Group for the final
25 determination regarding whether an investigative lead/task will be assigned.)
 - 26 ■ Non-actionable information that constitutes intelligence, but does not require
27 the assignment of an investigative lead/task by the Investigative Operations
28 Group. (Absent unusual circumstances, this information will be
29 communicated to the Investigative Operations Group.)
- 30 ○ Assessed by performing the appropriate databases/records queries.
- 31 ○ Analyzed to determine whether the incoming information is related to any existing
32 information.
- 33 ○ Disseminated to all of the appropriate Intelligence/Investigations Section personnel.

34
35 Operations security, operational security and information security activities include, but are not
36 limited to, the following:

- 37 ○ Ensure operations security, operational security and information security procedures
38 and activities are implemented.
- 39 ○ Ensure classified information is disseminated to personnel who have the required
40 clearance, access and “need to know” and is disseminated in compliance with all
41 associated caveats/restrictions (e.g., Grand Jury information restrictions).
- 42 ○ Ensure sensitive information is disseminated to appropriate and authorized personnel
43 who have the required “need to know,” and in strict compliance with all of the
44 applicable restrictions.
- 45 ○ Confer with the Command and General Staff to ensure the confidentiality and

1 security of intelligence/investigations activities are not compromised.

2
3 The information management function involves, but is not limited to, the following activities:

- 4 ○ Ensure tactical and strategic intelligence/investigations information is appropriately
5 collected.
 - 6 ■ Ensure intelligence requirements are used to manage and direct intelligence
7 collection efforts.
 - 8 ■ Ensure database/record queries are performed.
 - 9 ■ Ensure language translation services are provided.
 - 10 ■ Ensure deciphering and decryption services are provided.
 - 11 ■ Notify and confer with appropriate subject matter experts.
 - 12 ■ Identify and collect intelligence/investigations information by monitoring the
13 media, the public, appropriate governmental agencies, nongovernmental
14 organizations and private sector entities/individuals.
- 15 ○ Ensure intelligence/investigations information is appropriately documented,
16 organized, evaluated, collated, processed, exploited and analyzed.
- 17 ○ Ensure intelligence information needs and requests for intelligence; intelligence gaps;
18 and standing and ad-hoc intelligence requirements are identified, documented,
19 analyzed, validated, produced and resolved, as applicable
- 20 ○ When applicable, ensure requests for intelligence/investigations information are made
21 to the appropriate governmental agencies, nongovernmental organizations, private
22 sector entities/individuals, the media, and the public.
- 23 ○ Ensure finished and, if appropriate, raw intelligence/investigations information is
24 documented and produced (e.g., records, data, warnings, situation reports, briefings,
25 bulletins, and/or assessments).
- 26 ○ When necessary, ensure unclassified or lesser classified “tearlines” or tearline reports
27 are produced regarding appropriate classified information.
- 28 ○ When necessary, ensure classified information and/or access controlled Sensitive
29 Compartmented Information (SCI) and/or caveated/restricted information is sanitized
30 in order to use the information to create and investigate leads/tasks, publish
31 intelligence products, prepare warrant applications and accusatory instruments, etc.
- 32 ○ Ensure intelligence/investigations information, documents, requirements and
33 products are appropriately disseminated.
- 34 ○ When applicable, ensure requests for intelligence/investigations information are
35 documented, analyzed, managed and resolved.

36
37 Depending upon the size, complexity, and scope of the Intelligence/Investigations Section, the
38 Intelligence Group Supervisor may activate one or more of the following positions. As the
39 configuration of the ICS organization is flexible, the IC/UC may choose to combine these
40 functions or create teams to perform these functions.

- 41 ○ Information Intake and Assessment Manager
- 42 ○ Requirements Coordinator
- 43 ○ Collection Coordinator
- 44 ○ Processing and Exploitation Coordinator
- 45 ○ Analysis and Production Coordinator
- 46 ○ Dissemination Coordinator

- 1 ○ Infrastructure Protection Coordinator
- 2 ○ Classified National Security Information Security Officer
- 3

4 **Forensic Group**

5 The Forensic Group will manage and direct the documentation, processing, collection, invoicing,
6 safeguarding, analyzing and storing of forensic evidence, which includes digital/multimedia
7 evidence. The Forensic Group will be responsible for managing crime scenes and for ensuring
8 that the proper types of analyses are performed on the forensic evidence. This analysis must take
9 place in the proper sequence by appropriate laboratory or analytical service providers.

10

11 The Forensic Group will be responsible for ensuring:

- 12 ○ The number and location of each of the crime scenes is identified and assessed and
13 that each is sufficiently large and properly configured.
- 14 ○ Each of the crime scenes is safeguarded and secured.
- 15 ○ Each of the crime scenes is documented, searched, processed, etc.
- 16 ○ Personnel processing crime scenes confer with the primary case investigator and
17 supervisor and other appropriate personnel (e.g., responders that were the first to
18 arrive at each crime scene.)
- 19 ○ Personnel processing crime scenes assess the safety hazards, confer with the Safety
20 Officer and when necessary, utilize the appropriate PPE and comply with all incident
21 related safety procedures.
- 22 ○ Post-blast crime scene operations and forensic debris operations are implemented,
23 when necessary.
- 24 ○ Forensic evidence contamination, alteration, loss and destruction are prevented.
- 25 ○ Crime scene reconstruction techniques are utilized, when necessary.
- 26 ○ Appropriate records are prepared regarding forensic evidence documentation,
27 searches, collection, invoicing, processing, submission to a laboratory, etc.
- 28 ○ Forensic evidence is examined and analyzed by the appropriate laboratory or
29 analytical service provider in the proper priority order, and the proper number/types
30 of examinations/analyses are performed in the correct sequence.
- 31 ○ Personnel processing crime scenes, the primary case investigator and/or supervisor
32 confer with the appropriate laboratory and analytical service provider personnel.
- 33 ○ Crime scenes are released at the appropriate time and are not prematurely released.

34

35 Depending upon the size, complexity, and scope of the Intelligence/Investigations Section, the
36 Forensic Group Supervisor may activate one or more of the positions below. As the
37 configuration of the ICS organization is flexible, the IC/UC may choose to combine these
38 functions or create teams to perform these functions.

- 39 ○ Crime Scene Coordinator
- 40 ○ Bomb Operations Coordinator
- 41 ○ CBRNE/HazMat Evidence Coordinator
- 42 ○ Forensic Evidence Analysis Manager (including digital/multimedia evidence)

43

44

1 **Medicolegal Group**

2 The Medicolegal Group will manage and direct intelligence/investigations activities involving
3 fatality management operations; and, decedents, and missing persons and unidentified persons
4 investigations. Additionally, the Group will participate in Family Assistance Center operations
5 to gather information regarding the decedents, missing persons and unidentified persons. As the
6 configuration of the ICS organization is flexible, the IC/UC may choose to combine these
7 functions or create teams to perform these functions.

8
9 The Medicolegal Group will be responsible for ensuring:

- 10 ○ Fatality management activities are implemented.
- 11 ○ Decedents, missing persons and unidentified persons reporting and tracking activities
12 are implemented.
- 13 ○ Decedents, missing persons and unidentified persons are investigated and identified,
14 and required notifications are made in an appropriate and timely manner in
15 coordination with the medical examiner/coroner.
- 16 ○ Information, data, records, images, objects and DNA reference samples regarding
17 decedents, missing persons and unidentified persons are collected at a Family
18 Assistance Center.
- 19 ○ Confirmation and/or pronouncement of death have occurred.

20
21 Depending upon the size, complexity, and scope of the Intelligence/Investigations Section, the
22 Medicolegal Group Supervisor may activate one or more of the following positions. As the
23 configuration of the ICS organization is flexible, the IC/UC may choose to combine these
24 functions or create teams to perform these functions.

- 25 ○ Fatality Management Investigative Coordinator
- 26 ○ Missing/Unidentified Persons Coordinator
- 27 ○ Family Assistance Center Coordinator

28
29
30 **Investigative Support Group**

31 The resource and support needs of the Intelligence/Investigations Section may require the use of
32 specialized personnel, equipment, vehicles, supplies and facilities. The Investigative Support
33 Group will work closely with the Command and General Staff, particularly the Logistics and
34 Planning Sections, to ensure that necessary resources and support are obtained for the
35 Intelligence/Investigations Section.

36
37 The Investigative Support Group, working in conjunction with the Logistics and Planning
38 Sections, will be responsible for ensuring that:

- 39 ○ An appropriate number of Intelligence/Investigations Section Staging Areas are
40 activated, when necessary.
- 41 ○ Personnel are dispatched to the designated Staging Area or off-incident location,
42 checked-in, equipped, instructed, assigned if applicable, relieved when necessary,
43 notified regarding subsequent appearances and eventually demobilized.
- 44 ○ Vehicles, aircraft, watercraft, equipment, supplies, radios, wireline/wireless
45 telephones, facsimile machines, Secure Telephone Equipment (STE), computers,

- 1 image capture devices and electronic surveillance equipment are obtained, distributed
- 2 and maintained.
- 3 ○ Facilities (including a mobile SCIF, when necessary), infrastructure, systems and/or
- 4 networks are provided.
- 5 ○ When applicable, food and beverages are provided.
- 6 ○ Technical and non-technical support is provided.
- 7 ○ Items and services that must be procured are requested in a timely manner.
- 8 ○ Appropriate records are maintained regarding support activities.
- 9

10 Depending upon the size, complexity, and scope of the Intelligence/Investigations Section, the
11 Investigative Support Group Supervisor may activate one or more of the following positions.
12 As the configuration of the ICS organization is flexible, the IC/UC may choose to combine these
13 functions or create teams to perform these functions.

- 14
- 15 1. One or more Staging Area Managers.
 - 16 a. Properly documents the appropriate information regarding all of the responding
 - 17 resources.
 - 18 b. Categorizes and separates all of the responding personnel based upon one or more
 - 19 of the following criteria:
 - 20 i. Agency jurisdiction and legal authority.
 - 21 ii. Personnel technical skills (e.g., crime scene technician, behavioral analyst,
 - 22 electronic surveillance technician, arson cause and origin investigator,
 - 23 bomb technician, forensic scientist, polygraph analyst, computer
 - 24 investigator).
 - 25 iii. Personnel non-technical skills (e.g., interrogation, interview, undercover,
 - 26 language, intelligence analyst, physical surveillance, juvenile offenses, data
 - 27 entry, administrative).
 - 28 iv. Personnel Clearance (e.g., Top Secret, Secret) and Access (one or more
 - 29 Sensitive Compartmented Information (SCI) programs.)
 - 30 v. Personnel Proficiency.
- 31 2. Intelligence/Investigations Section Work Area Manager.
 - 32 a. Ensure the Intelligence/Investigations Section Work Area is maintained in an
 - 33 orderly manner; and all of the facilities, accommodations, infrastructure and
 - 34 service related requirements are satisfied.
- 35 3. Resource Coordinator.
 - 36 a. If a significant number of resources are required, work directly with counterparts
 - 37 in the Logistics Section to order resources and in the Planning Section to account
 - 38 for all resources.
- 39 4. Communications Coordinator.
 - 40 a. Ensure all appropriate radio channels are monitored at the
 - 41 Intelligence/Investigations Section work area.
 - 42 b. Ensures the Intelligence/Investigations Section Communications Plan is prepared
 - 43 and updated, and is disseminated to the Logistics Section.
 - 44 c. Ensures required communication devices and equipment are distributed,
 - 45 maintained and repaired when necessary.
- 46 5. Security Coordinator.

- 1 a. When necessary, assign personnel to thoroughly search the area where the
- 2 Intelligence/Investigations Section work area is situated for force
- 3 protection/security, health and safety hazards.
- 4 b. Ensures that appropriate security measures are implemented at the
- 5 Intelligence/Investigations Section work area and other appropriate areas (e.g.,
- 6 crime scenes, investigative scenes).
- 7 c. When necessary, ensure identification credentialing/badging procedures are
- 8 implemented.

1 **Acronym List**

2

CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
EOP	Emergency Operations Plan
ERFOG	Emergency Responder Field Operations Guide
FBI	Federal Bureau of Investigation
FOG	Field Operations Guide
FOUO	For Official Use Only
HazMat	Hazardous Materials
IAP	Incident Action Plan
IC	Incident Commander
ICS	Incident Command System
IIFOG	Intelligence/Investigations Function Field Operations Guide
JOC	Joint Operations Center
MACS	Multiagency Coordination Systems
ME/C	Medical Examiner/Coroner
NIMS	National Incident Management System
NOFORN	Not Releasable to Foreign Nationals
OPSEC	Operations Security
ORCON	Dissemination and Extraction of Information Controlled by Originator
PPE	Personal Protective Equipment
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
UC	Unified Command

3

1 **Definitions**

2
3 **Analysis** – The comprehensive and systematic examination, assessment and evaluation of
4 collected, processed and exploited information/data in order to identify significant facts and
5 derive valid conclusions.

6
7 **Branch** – The organizational level having functional or geographical responsibility for major
8 aspects of incident operations. A Branch is organizationally situated between the Section Chief
9 and a Division, Group, and/or Units. Branches are identified by the use of roman numerals or by
10 functional area.

11
12 **Classified National Security Information** (also referred to as "classified information") – Any
13 data, file, paper, record, or computer screen containing information associated with the national
14 defense or foreign relations of the United States and bearing the markings: confidential, secret, or
15 top secret. This information has been determined pursuant to Executive Order 12958 or any
16 predecessor order to require protection against unauthorized disclosure and is marked
17 (confidential, secret, or top secret) to indicate its classified status. It is also referred to as
18 classified information.

- 19 • Confidential: Information, the unauthorized disclosure of which reasonably could be
20 expected to cause damage to the national security that the original classification authority
21 is able to identify or describe.
- 22 • Secret: Information of which the unauthorized disclosure could reasonably be expected to
23 cause serious damage to the national security that the original classification authority is
24 able to identify or describe.
- 25 • Top secret: Information of which the unauthorized disclosure could reasonably be
26 expected to cause exceptionally grave damage to the national security that the original
27 classification authority is able to identify or describe.

28
29 **Collection** – Gathering information through approved techniques to address and/or resolve
30 Intelligence Requirements. The sources of information that are used during the Collection step of
31 the Intelligence Cycle include HUMINT, SIGINT, IMINT, OSINT, MASINT.

32
33 **Command Staff** – Consists of Public Information Officer, Safety Officer, Liaison Officer, and
34 other positions as required, who report directly to the Incident Commander. They may have an
35 assistant or assistants, as needed.

36
37 **Crime Scene** – An area or areas that contain physical evidence that may have forensic,
38 investigative, demonstrative or other probative value. Crime Scenes include “Remains Collection
39 Areas”/“Body Collection Points” where the decedents are gathered for processing and
40 safeguarding.

41
42 **Decedents** – A deceased person, including portions of remains from that person.

43
44 **Director of National Intelligence (DNI)** – Position created pursuant to the Intelligence Reform
45 Act of 2004. The DNI has “executive authority” to oversee the U.S. Intelligence Community.

1
2 **Dissemination** – The timely release, distribution and delivery of raw intelligence and finished
3 intelligence products to the appropriate recipients in compliance with defined protocols.
4 Dissemination is the general policy and rule; and, raw and finished intelligence and information
5 will be disseminated unless the dissemination is legally or procedurally prohibited. These
6 prohibitions, also known as Dissemination restrictions/caveats, are not a level of Classification,
7 but they are used in conjunction with the appropriate Classification level and caveat the sharing,
8 distribution and delivery of intelligence/information. Some examples of Dissemination
9 restrictions/caveats are:

- 10 • ORCON (Dissemination and Extraction of Information Controlled by Originator) – no
11 further dissemination can occur without the prior approval of the originator
- 12 • NOFORN (Not Releasable to Foreign Nationals) – may not be provided, in any form, to
13 foreign governments, international organizations, coalition partners, foreign nationals or
14 immigrant aliens
- 15 • REL TO – authorized for release to... (specify country)
- 16 • RELIDO – Releasable by Information Disclosure Officer
- 17 • FISA – Foreign Intelligence Surveillance Act
- 18 • Grand Jury Information – protected by Federal and State statute
- 19 • Taxpayer Information – protected by Federal statute

20
21 **Family Assistance Center** – Is established to facilitate the exchange of information between
22 disaster responders and the family members and friends of decedents, those injured, and those
23 missing/unidentified. Family Assistance Center personnel address the immediate emotional
24 needs of the victim’s families and friends and provide accurate and timely information in an
25 appropriate setting and compassionate manner. The Family Assistance Center must also address
26 the basic physical needs of these family members and friends of victims, including food, shelter
27 transportation, internet access, telephone, child care, language translation, disaster mental health
28 services, and emergency medical services, if necessary.

29
30 **Force Protection** – Protecting responders from security hazards involving one or more persons,
31 devices, objects, animals, conditions or situations (e.g., hostile person; sniper; hostage taker;
32 barricaded person; fugitive; emotionally disturbed person; non-hostile unauthorized person;
33 explosive device or substance; CBRNE/HazMat source, dissemination device or release; person
34 conducting intelligence collection, surveillance or reconnaissance activities/operations; firearm;
35 aggressive animal; dangerous device, weapon or object).

36
37 **Forensics** – The use of science and technology to investigate and establish facts in criminal or
38 civil courts of law.

39
40 **General Staff** – A Group of incident management personnel organized according to function
41 and reporting to the Incident Commander. The General Staff normally consists of the Operations
42 Section Chief, Planning Section Chief, Logistics Section Chief, Finance/Administration Section
43 Chief, and, if required, Intelligence/Investigations Section Chief.

1 **Group** – Established to divide the incident management structure into functional areas of
2 operations, Groups are composed of resources assembled to perform a special function not
3 necessarily within a single geographic division.

4
5 **Human Intelligence (HUMINT)** – Intelligence information acquired by human sources through
6 covert and overt collection techniques.

7
8 **Imagery Intelligence (IMINT)** – The collection, analysis and interpretation of conventional,
9 analog and digital image information/data.

10
11 **Incident Action Plan (IAP)** – An oral or written plan containing general objectives reflecting
12 the overall strategy for managing an incident. It may include the identification of operational
13 resource and assignments. It may also include attachments that provide directions and important
14 information for management of the incident during one or more operational periods.

15
16 **Incident Command Post (ICP)** – The field location where the primary functions are performed.
17 The ICP may be co-located with the incident base or other incident facilities.

18
19 **Incident Objectives** – Statements of guidance and direction needed to select appropriate
20 strategy(s) and the tactical direction of resources. Incident objectives are based on realistic
21 expectations of what can be accomplished when all allocated resources have been effectively
22 deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow
23 strategic and tactical alternatives.

24
25 **Information Security** – Refers to the policies, practices and procedures that are applied to
26 information systems to ensure that data and information that is held within or communicated
27 along those systems is not vulnerable to inappropriate or unauthorized discovery, use, access,
28 export or modification and that the networks that are used to store, process or transmit
29 information are kept operational and secure against unauthorized access.

30
31 **Intelligence** – Can be defined slightly differently depending on the agency or organization of
32 focus, but generally speaking can be defined as, the combination of credible information with
33 quality analysis—information that has been evaluated and from which conclusions have been
34 drawn.

- 35 • **Raw Intelligence** – Collected information/data that has not been processed, integrated,
36 analyzed, evaluated, and interpreted.
- 37 • **Finished Intelligence** – The product resulting from the processing, exploitation,
38 integration, evaluation, analysis and interpretation of collected information & data.
- 39 • **Strategic Intelligence** – Information tailored to support the planning and execution of
40 agency-wide intelligence and investigative programs, and the development of long term
41 policies, plans and strategies.
- 42 • **Tactical Intelligence** – Information that directly supports on-going operations and
43 investigations.

44
45 **Intelligence Gap** – An unanswered question(s) regarding a criminal, cyber or national security
46 issue or threat.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46

Intelligence Information Need – Describes information and/or intelligence needed to eliminate intelligence gaps.

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 information and/or intelligence to collect, report, produce and disseminate. Intelligence requirements provide the questions that you ask your HUMINT, and the information that you seek from your SIGINT, IMINT and OSINT. 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. Ad hoc intelligence requirements normally involve a particular investigation or incident and are resolved in short order.

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

Investigative Scene – An area or areas where investigative information may be obtained by identifying/interviewing witnesses; performing non-technical and technical canvasses; examining conventional, analog and digital investigative evidence (e.g., documents/text, images/photos, audios, data; utilizing eyewitness identification techniques). Investigative Scenes include:

- Casualty collection areas where ill/injured persons are gathered for emergency triage, treatment, and/or transportation to a health care facility.
- Areas where decontamination operations are conducted.
- Evacuation assembly areas/facilities.
- Shelter-in-place facilities/locations, when appropriate.
- Personnel checkpoints.
- Vehicle roadblocks.
- Traffic Control Points and Access Control Points.
- Family Assistance Centers.
- Mass transit facilities/conveyances.
- Health care facilities, when appropriate.

Medical Examiner – A physician who is appointed by the government to oversee and/or perform medicolegal death investigations.

Medicolegal – Of, relating to, or concerning both medicine and law.

Medicolegal Death Investigator – A professional having the legal authority to investigate deaths for a medicolegal (medical examiner/coroner) jurisdiction, who performs scene investigations, collects evidence and develops decedents’ medical and social histories to assist the medical examiner/coroner in determining the cause and manner of death. Medicolegal death investigators should have a combination of education and skills encompassing areas of medicine and law.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46

Medicolegal Investigation- The collection of data, photographs, evidence, witness interviews, external examination of the body at the scene, and other forensic information and analysis that will contribute to the determination of cause and manner of death, reconstruction of the accident or crime scene, and support the provision of survivability factors. The medicolegal investigation falls within the exclusive purview of the Medicolegal Authority operating at the scene of an incident.

Missing Persons – Persons whose whereabouts are unknown to family or friends following an incident.

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 required in order to permit that individual to perform their official duties. The determination is not made solely by virtue of an individual's office, position, or security clearance level.

Nongovernmental Organizations – An entity with an association that is based upon the interests of its member individuals or institutions; and, that is not created by a governmental agency, but may work cooperatively with any relevant governmental agencies. Non-governmental organizations serve a public purpose and not a private benefit. Examples of non-governmental organizations include faith based charity organizations, the Salvation Army and the American Red Cross.

Non-technical canvasses –Involve traditional canvasses for persons and vehicles in order to identify witnesses and sources of information. Non-technical canvasses may involve residential and commercial buildings, schools, recreational sites, mass transit facilities, crime scenes and investigative scenes.

Open Source (OSINT) – Publicly available information and unclassified information that has limited public distribution or access.

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, counter surveillance measures, counter intelligence methods, undercover officers, cooperating witnesses and informants.

Operations Security (OPSEC) – A process to identify, control and protect information that is generally available to the public regarding sensitive or classified information and activities that could be used by a potential adversary to the disadvantage of a governmental agency, non-governmental organization or private entity/individual. Application of the OPSEC 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, non-governmental organization 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?

- 1 3. Analyze direct and indirect vulnerabilities: how might the adversary collect the
2 information that must be protected?
- 3 4. Assess the risk: balance the cost of correcting the vulnerabilities as compared to the cost
4 of losing the information that must be protected.
- 5 5. Implement appropriate countermeasures: eliminate or reduce vulnerabilities, and/or
6 disrupt the adversary's collection capabilities and efforts and/or prevent the accurate
7 interpretation of the information that must be protected.

8
9 **Prevention** – Actions to avoid an incident or to stop an incident from occurring. Prevention
10 involves applying intelligence and other information to a range of activities that may include
11 such countermeasures as deterrence operations; inspections; surveillance, security operations;
12 investigations to determine the full nature and source of a threat; and, public health surveillance
13 and laboratory analysis procedures. Prevention also involves specific law enforcement operations
14 aimed at deterring, preempting, interdicting or disrupting illegal activity; and, apprehending
15 potential perpetrators and bringing them to justice.

16
17 **Processing and Exploitation** – Converting raw information/data into formats that can be
18 efficiently and effectively used by executives, managers, analysts and investigators. Examples of
19 Processing and Exploitation include:

- 20 • Imagery interpretation
- 21 • Data conversion and correlation
- 22 • Document and eavesdropping translations
- 23 • Key Word searches on seized data
- 24 • Facial Recognition searches involving image capture systems, records, databases, etc
- 25 • Data Mining in seized or open source databases
- 26 • Decryption of seized or intercepted data

27
28 **Production** – The documentation and creation of finished and/or raw intelligence/information
29 including records, data, warnings, reports, briefings, bulletins, biographies, assessments, in a
30 conventional, analog and/or digital format utilizing text, images, audios and data.

31
32 **Sensitive Compartmented Information (SCI)** – A restricted access control system. It is a level
33 of access to classified information compartments/programs, and not a level of Classification. The
34 SCI access control system applies to all three levels of classified information (Top Secret, Secret,
35 Confidential). SCI access is usually based upon the sensitivity of the involved sources and/or
36 methods.

37
38 **Sensitive Compartmented Information Facility (SCIF)** – An accredited area, room, group of
39 rooms, or installation where SCI may be stored, used, discussed, and/or electronically processed.
40 SCIF procedural and physical measures prevent the free access of persons unless they have been
41 formally indoctrinated for the particular SCI authorized for use or storage within the SCIF.

42
43 **Signals Intelligence (SIGINT)** – Intelligence information derived from the interception of
44 transmitted electronic signals.

45

1 **Situation Board** – Large sheets of paper or white boards that are affixed to walls visible to those
2 working an intelligence/investigations operation. These boards give individuals immediate
3 access to crucial information regarding the incident at hand. They also provide other crisis
4 management team members a commanding view of information as it is processed.

5
6 **Staging Area** – Established for the temporary location of available resources. A Staging Area
7 can be any location in which personnel, supplies, and equipment can be temporarily housed or
8 parked while awaiting operational assignment.

9
10 **Tactical** – Of or relating to small-scale actions serving a larger purpose; made or carried out with
11 only a limited or immediate end in view.

12
13 **Tearline Report** – Contains information that has been declassified or information that is at a
14 reduced/downgraded Classification level as compared to the original report from which the
15 Tearline report is generated/produced. A Tearline report is produced by redacting, paraphrasing,
16 restating or generating in a new form the classified information contained in the original report in
17 such a manner that the previously classified information is now either declassified or is at a
18 reduced/downgraded Classification level.

19
20 **Technical canvasses** – Technical canvasses involve canvasses for electronic devices in order to
21 identify witnesses and sources of information. Technical canvasses may involve electronic image
22 capture devices (still, video, CCTV), electronic banking transaction devices (Automated Teller
23 Machine), electronic financial transaction devices (credit card, debit card, social services card,
24 stored value card), electronic travel transaction devices (Metro Card, EZ Pass, airline ticket,
25 railroad ticket), electronic access/egress control devices (identification card reader, proximity
26 card reader, biometric card reader), cell sites, pay phones, internet cafes.

27
28 **Technical Specialist** – Personnel with special skills that can be used anywhere within the ICS
29 organization. No minimum qualifications are prescribed, as technical specialists normally
30 perform the same duties during an incident that they perform in their everyday jobs, and they are
31 typically certified in their fields or professions.

32
33 **Threat** – An indication of possible violence, harm or danger.

34
35 **Unidentified Persons** – Includes those persons, both injured and deceased, who require the
36 application of scientific methods to verify their identification.

37
38 **United States Intelligence Community** – A federation of executive branch agencies and
39 organizations that work separately and together to conduct intelligence activities necessary for
40 the conduct of foreign relations and the protection of the national security of the United States.
41 The US Intelligence Community functions as a single corporate enterprise, supporting those who
42 manage the nation's strategic interests – political, economic, and military. The US Intelligence
43 Community is comprised of the following sixteen (16) entities:

- 44 • Central Intelligence Agency
- 45 • Federal Bureau of Investigation
- 46 • National Security Agency

DRAFT: Intelligence/Investigations Function Guidance Document
Version 3 (February 2008)

- 1 • National Reconnaissance Office
- 2 • National Geospatial Intelligence Agency
- 3 • Department of State
- 4 • Department of Homeland Security
- 5 • Department of Energy
- 6 • Defense Intelligence Agency
- 7 • Army
- 8 • Air Force
- 9 • Navy
- 10 • Marines
- 11 • Coast Guard
- 12 • Department of Treasury
- 13 • Drug Enforcement Administration
- 14