

**Department of Homeland Security
Office of Intelligence and Analysis**

Intelligence Operations

SOP Number: FO-001

Revision: 00

Issue Date: 08/24/2015

STANDARD OPERATING PROCEDURE: INCIDENT ACTION PLANNING

I. Purpose and Scope

This handbook provides Field Operations Division (Field Ops) personnel, leadership, and partners a resource to assist in developing planning materials necessary to prepare for, support, and respond to situations requiring Field Ops information and intelligence operations support to DHS/I&A Leadership, State, local, tribal, territorial, and private sector (SLTTP), DHS Intelligence Enterprise (DHS IE), and other federal partners. This handbook establishes the roles, responsibilities, processes, and procedures necessary to develop and implement Incident Action Plan (IAP) materials. This handbook applies to all Field Ops personnel, leadership, contractors, and inter/intra-agency liaisons/detailees assigned to Field Ops. The handbook is "For Official Use Only" (FOUO) and can be shared with State, local, tribal, territorial, and private sector (SLTTP) and federal partners as needed.

Field Ops is a unique I&A organization in that field and HQ personnel have extensive arrays of information sharing and intelligence operations responsibilities; a wide range of SLTTP, DHS IE, and federal partners; potential personnel bandwidth and availability challenges; and requirements to rapidly adjust operational postures based on partner needs, threats, and incidents. As such, a regional IAP provides a process and strategy with which Regional Directors (RD) can effectively support partners and operations, manage and direct regional personnel and resources, and coordinate with Field Ops and I&A leadership.

An IAP is a written plan that defines incident objectives and the capabilities necessary to manage Field Ops activities during specific situations. For the purposes of Field Ops, and consistent with the National Incident Management System (NIMS), IAPs are scalable to meet, respond to, and support Field Ops mission requirements. For example, an Intelligence Officer (IO) may develop an IAP that is able to support a local Special Event Assessment Rating (SEAR) 4 special event and fully capable of conducting necessary Field Ops missions. In the event a major unexpected incident occurs the IO can coordinate with the RD to expand the IAP and assign capabilities to other regional personnel. The regional standing IAP or the SEAR 4 IAP may be tailored to best assign capabilities based on the situation, requirements, and available resources.

II. Definitions

- A. Field Operations Division Incident Action Plan Capabilities: Activities or functions that should be considered and/or conducted depending on the nature, scope, and complexity of the incident. Field Ops personnel are responsible for being able to conduct these capabilities during incident operations. The following are Field Ops' common IAP capabilities:
1. Area of Responsibility (AOR)/Regional Intelligence Support Requirements: Identify, submit, and track intelligence support requests (briefs, products, etc.) submitted to I&A HQ for action.
 2. AOR/Regional Collection Requirements: Identify and manage intelligence collection requirements originating from AOR, regional, or HQ partners.
 3. Request for Information (RFI) Management: Excluding Collection Requirements, manage, track, and direct information flow to include situational awareness, requests for information (RFIs), requests for assistance (RFAs), etc.
 4. Product Development: Draft and submit situation reports, Intelligence Information Reports (IIR), Field Intelligence Reports (FIR), etc.
- B. Incident Action Plan (IAP): A written plan that defines incident objectives and the capabilities necessary to manage Field Ops activities during specific situations. For the purposes of Field Ops, and consistent with the National Incident Management System (NIMS), IAPs are scalable to meet, respond to, and support Field Ops mission requirements.
- C. Incident Command System IAP Forms: Forms/templates used to develop, maintain, and implement Field Ops IAPs.
- D. National Special Security Event (NSSE): National or international, government or privately sponsored events or gatherings of national significance that are deemed to be potential terrorist targets requiring the counterterrorism capabilities of the Federal government. Some events categorized as NSSEs include presidential inaugurations, major international summits held in the United States, major sporting events and presidential nominating conventions. Additionally, some events, such as the State of the Union Addresses and State funerals in Washington, DC are pre-designated as NSSEs, and other events may be designated by the President or his representative, the Secretary of DHS if warranted by certain factors and considerations.
- E. Special Event Assessment Rating (SEAR) Special Events: Preplanned special events below the level of NSSEs which have been submitted via

the annual National Special Event Data Call. The majority of these events are state and local events that may require support augmentation from the federal government.”

III. Responsibilities

These roles and responsibilities only apply to regional IAP requirements; existing roles and responsibilities still apply to Field Ops personnel.

A. Field Operations Leadership

Manage Field Ops’ division operations in support of national, regional and field incident management operations to include:

1. Provide requirements, guidance, and direction to RDs for inclusion into steady-state, special event, or incident-specific IAPs.
2. Provide Intelligence Operations (Intel Ops) IAP products, Intel Ops and Field Ops leadership Critical Information Requirements, significant HQ Operations Schedule activities, etc. to RDs or other designated Field Ops personnel.
3. Review and assess reporting and requests in the event of IAP execution.
4. Coordinate with impacted RD and other RDs to support incident operations and provide guidance/situational awareness to Field Ops personnel in non-impacted locations.
5. Direct Field Ops HQ personnel and coordinate with Intel Ops leadership on operational, resource, and mission requirements, challenges, etc.
6. Direct, manage, coordinate, or de-conflict HQ and/or field operational or IAP communications, coordination, or other mission requirements.

B. Regional Directors

Manage and direct regional I&A personnel. RDs represent and convey I&A, Intel Ops, and Field Ops leadership guidance and requirements to IOs.

1. Receive IAP and incident management requirements, guidance, and direction from Field Ops leadership.

2. Develop and maintain a regional IAP for use in potential/actual incident operations.
3. Provide direction and guidance to IOs, Senior Reports Officers (SRO), and Reports Officers (RO) in developing and maintaining AOR or special event IAP requirements.
4. Serve as the primary regional communications and coordination point for regional incident management/IAP operations.
5. Manage and assign regional personnel to IAP work assignments (ICS-204).
6. Be prepared to support other Field Ops regions.

C. Intelligence Officers and Reports Officers

Serve as I&A's direct, field-level representatives and key DHS and I&A intelligence support conduits to SLTTPS, DHS IE, and other partners.

1. Develop and implement IAPs to support SLTTP, DHS IE, and federal partners as needed, warranted, or otherwise directed by their RD.
2. Report changes in availability status to their RD.
3. Be prepared to execute IAP assignments (ICS-204).

D. On-site Intelligence Officer

These are Field Ops personnel directly involved in supporting event preparedness efforts and developing/executing an IAP or Field Ops personnel directly involved in supporting threat/incident operations requiring support from the RD and regional IAP.

1. Draft and execute IAPs for special events with established command centers requiring on-sight or virtual Field Ops support.
2. Serve as the primary event manager for Field Ops incident management functions.
3. Coordinate with the RD on the need for additional support and for the expansion of the AOR-specific-IAP or Regional IAP if required by the threat or incident scope.

IV. Standard Operating Procedures

Field Ops IAP methods leverage several modified Incident Command System (ICS) forms. IAP execution is managed and directed by the On-site IO, the RD, or the RD's designee. This section addresses IAP Development, Dissemination, Execution, and Maintenance.

A. Field Operations Division Incident Action Plan Capabilities

These are activities or functions that should be considered and/or conducted depending on the nature, scope, and complexity of the incident or event. Field Ops personnel are responsible for being able to conduct these capabilities during incident/IAP operations. The following are Field Ops' common IAP capabilities:

1. *Area of Responsibility (AOR)/Regional Intelligence Support Requirements:* Identify, submit, and track intelligence support requests (briefs, products, etc.) submitted to I&A HQ for action.
2. *AOR/Collection Requirements:* Identify and manage intelligence collection requirements originating from AOR, regional, or HQ partners.
3. *Request for Information (RFI) Management:* Excluding Collection Requirements, manage, track, and direct information flow to include situational awareness, RFIs, requests for assistance (RFA), etc.
4. *Product Development:* Draft and submit situation reports, Intelligence Information Reports (IIR), Field Intelligence Reports (FIR), etc.

B. IAP Development

The implementation of this IAP SOP will be applied but not limited to the following situations/events. RDs may develop or direct regional personnel to develop additional IAPs at his/her discretion.

1. A steady-state regional IAP developed and maintained by the RD for use during an emerging threat or incident.
2. SLTT special events, regardless of a federal SEAR or National Special Security Event (NSSE), requiring on-sight or virtual Field Ops support.

3. As directed by Field Ops leadership.

The following sections identify the standard/required modified ICS forms (modified to accommodate Field Ops' unique mission space) necessary for a complete Field Ops IAP.

1. **ICS-201: Incident Briefing (Annex A):** Provides Field Ops and partners with basic information regarding the incident situation and the Field Ops resources allocated. Key elements include:
 - a. Incident Name: This can be whatever the IAP developer chooses so long as it is easily understood by personnel reviewing the IAP.
 - b. Situation Summary: Provides general awareness on the threat/incident that is relevant to regional Field Ops mission space and partner needs. If the situation is related to a classified product (Joint Intelligence Bulletin, threat brief, etc.), simply reference the product and share it with cleared partners as a supplemental document.
 - c. Operations Schedule: This identifies and articulates key activities (meetings, conference calls, shift schedules, SVTCs, reporting timelines, etc.) relevant to Field Ops.
 - d. Current/Planned Objectives: Objectives drive Field Ops activities throughout the event.
 - e. Objective development includes input and requirements identified by I&A/Field Ops leadership, Intelligence Operations IAPs, and RDs. Regional objectives should include Field Ops relationships and mission needs of SLTTP, DHS IE, and other federal partners.
 - f. Organizational Chart: The organization chart identifies assigned personnel, assigned positions and chains of command.

2. **ICS-202: Incident Objectives** (*Annex B*): Describes the basic incident strategy, incident objectives, command emphasis/priorities, and safety considerations. Key elements include:
 - a. Incident Name: Use the same name established in the ICS-201.
 - b. Operational Period: This is the time scheduled for executing a given set of operations to support IAP objectives. The Operational Period can cover the entire event time frame (days) or into consecutive Operational Periods (every 12 or 24 hours) throughout the duration of the event. IAPs should use AOR-specific time zones.
 - c. Objectives: Use the same objectives established in the ICS-201.
 - d. Operational Period Command Emphasis: This section identifies the priorities for the operational period. This is not a narrative of the objectives but a discussion about where to place emphasis if there are needs to be prioritized.
3. **ICS-204: Assignment List** (*Annex C*): Informs leadership and partners of IAP assignments. Key elements include:
 - a. Incident Name: Use the same name established in the ICS-201.
 - b. Operational Period: Use the same name established in the ICS-202.
 - c. Chain of Command: This section identifies key IAP leadership and contact information.
 - d. Resources Assigned: This section identifies Field Ops or other DHS/I&A personnel and contact information supporting the IAP.
 - e. Work Assignments: This section identifies capabilities, functions, assignments, etc. necessary to achieve IAP objectives within the designated operational period. The following work assignments are required for all Field Ops IAPs; RDs may add others as needed.

4. **ICS-205: Communications Plan** (Annex D): Provides contact information for Field Ops personnel involved in IAP preparedness and/or execution or directly/indirectly providing support. Key elements include:
- a. Incident Name: Use the same name established in the ICS-201.
 - b. Operational Period: Use the same name established in the ICS-202.
 - c. Key Partners: This section identifies all other key partners and contact information, command centers, DHS IE, and other federal partners. This also includes key I&A elements (Intelligence Watch, analytical divisions, National Operations Center (NOC), etc.)

** The Field Ops roster can be added as an attachment if needed.*

C. IAP Dissemination

All Field Ops IAPs, when completed or updated, should be disseminated to personnel with an IAP role, Field Ops HQ via the (b) (6), (b) (7)(E)@hq.dhs.gov distribution list, and I&A's Intelligence Watch at (b) (6), (b) (7)(E)@hq.dhs.gov. IAPs may be disseminated to other Field Ops regions or I&A elements as needed. Dissemination beyond I&A should be coordinated through respective RDs and Field Ops leadership.

Special event IAPs are largely influenced by the fluid nature of preparedness planning and coordination. **Final draft IAPs must be disseminated as instructed above no earlier than two weeks prior to the scheduled event.** Updated IAPs after this point should be disseminated as needed.

D. IAP Execution

Field Ops IAPs will be executed in accordance with the stated IAP chain of command, objectives, assignments, etc. Implemented IAPs will be modified or updated as required by incident operations, the RD, or Intel Ops/Field Ops leadership and mission requirements.

E. IAP Maintenance

Steady-state regional IAPs should be reviewed and updated at least once per year and, in addition to dissemination to the above recipients, be saved to the Field Ops Homeland Security Information Network (HSIN) Community of Interest (COI) within their regional folder.

V. Questions

Questions regarding this SOP should be addressed to the I&A Field Operations Division.

Appendix A: ICS-201 – Incident Briefing Template

Appendix B: ICS-202 – Incident Objectives Template

Appendix C: ICS-204 – Incident Assignment Template

Appendix D: ICS-205 – Incident Communication Plan Template

Appendix E: Special Event Background Information

(b) (6)

Kurt J. Reuther

Deputy Under Secretary of Intelligence Operations

8/24/15
Date

APPENDIX A: ICS-201 – INCIDENT BRIEFING TEMPLATE

1. Incident Name:

This can be whatever the IAP developer chooses so long as it is easily understood by personnel reviewing the IAP.

2. Date/Time Initiated:**3. Situation Summary:**

Provides general awareness on the threat/incident that is relevant to regional Field Ops mission space and partner needs. If the situation is related to a classified product (Joint Intelligence Bulletin, threat brief, etc.), simply reference the product and share it with cleared partners as a supplemental document.

4. Operations Schedule

This identifies and articulates key activities (meetings, conference calls, shift schedules, SVTCs, reporting timelines, etc.) relevant to Field Ops.

Time	Activity	Participant(s)	Location

5. Current and Planned Objectives:

Objectives drive Field Ops activities throughout the event. Objective development includes input and requirements identified by I&A/Field Ops leadership, Intelligence Operations IAPs, and RDs. Regional objectives should include Field Ops relationships and mission needs of SLTTP, DHS IE, and other federal partners.

6. Organizational Chart:

The organization chart identifies assigned personnel, assigned positions and chains of command.

APPENDIX B: ICS-202 – INCIDENT OBJECTIVES TEMPLATE

1. Incident Name: <i>Use the same name established in the ICS-201.</i>	2. Operational Period: Date from: Date To:
3. Objectives <i>Use the same objectives established in the ICS-201.</i>	
4. Operational Period Command Emphasis <i>This section identifies the priority subjects and capabilities for the operational period.</i> <u>General</u> • <u>I&A Operational Period Concept of Operations</u> • <u>Critical Information Requirements (CIRs)</u> • <u>Staff Accountability</u> • <u>AOR/Regional Intelligence Support Requirements:</u> • <u>AOR/Regional Collection Requirements</u> • <u>RFI Management:</u> • <u>Product Development:</u> • <u>Communications & Coordination</u> •	

APPENDIX C: ICS-204 – INCIDENT ASSIGNMENT TEMPLATE

1. Incident Name: <i>Use the same name established in the ICS-201.</i>	2. Operational Period: Date from: Date To:	
3. Chain of Command – Key IAP leadership		
Position	Name	Contact Information
		Work: Cell: E-mail: HSDN:
		Work: Cell: E-mail: HSDN:
4. Resources Assigned – Field Ops personnel or other DHS/I&A personnel assigned to support the IAP.		
Position	Name	Contact Information
		Work: Cell: E-mail: HSDN:
		Work: Cell: E-mail: HSDN:
		Work: Cell: E-mail: HSDN:
6. Work Assignments – This section identifies the capabilities assigned to IAP personnel necessary to achieve IAP objectives within the designated operational period. The following work assignments are required for all Field Ops IAPs; RDs may add others as needed.		
General: <i>Assignments that apply to all</i>		
Name	Assignment(s)	
	Location: Hours: Assignment: Key Products:	
	Location: Hours: Assignment: Key Products:	
	Location: Hours: Assignment: Key Products:	

APPENDIX D: ICS-205 – INCIDENT COMMUNICATION PLAN TEMPLATE

1. Incident Name: <i>Use the same name established in the ICS-201.</i>	2. Operational Period: Date from: Date To:	
4. Operations Personnel		
Position	Name	Contact Information
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:
		Work: Cell: E-mail:

APPENDIX D: ICS-205 – SPECIAL EVENT BACKGROUND INFORMATION

The information below is intended to provide Field Operations personnel a general understanding of the special event process so they can understand and be better prepared to support/inform SLTT partners, contribute to the federal special event communication and coordination effort; and conduct the necessary Field Operations planning activities.

Special Events and SEAR Ratings

Special events are defined as preplanned events which have been submitted via the annual National Special Event Data Call by State Administrative Agencies or submitted for evaluation as determined by SLTT partners. Typically in late summer/early fall, the Special Event Working Group (SEWG) issues a data call to State Administrative Agencies requesting the list of special events for the upcoming year. States are free to provide the number and types of special events they see fit but must include specific data points to allow the SEWG to determine and assign a Special Event Assessment Rating (SEAR). *States can also provide new special event nominations throughout the year in the event a new event is identified or data points have changed that could impact the SEAR rating.*

The SEAR rating scale consists of five levels; level one being the highest. SEAR ratings are based on a risk assessment methodology which provides an objective, facts-based determination. The SEWG is responsible for formally assigning SEAR ratings.

SEAR Level	Definition	Examples
1	- Significant national and/or international importance - May require extensive federal interagency support	- Super Bowl - United Nations General Assembly
2	- Significant events with national and/or international importance - May require some national-level federal support	- Boston Marathon - DC Fourth of July
3	- Events of national and/or international importance - Require only limited federal support	- Coca Cola 600 - Rolling Thunder
4	- Limited national importance - Handled at the State and local level	Big 10 Football Championship
5	Events that may be nationally recognized but generally have local or State importance	- Lepre-Con Festivities - West Orange (NJ) St. Patrick's Day Parade

National Special Security Events

NSSEs are different in that a State or Territory Governor must submit a NSSE designation request to the Secretary for the Department of Homeland Security. If/When a NSSE is designated, per PDD-63, the U.S. Secret Service is the lead federal agency.

Federal Coordinator

Federal Coordinators (FC) are designated by the Secretary to serve as the Secretary's representative for NSSEs (U.S. Secret Service), SEAR 1, and select SEAR 2 events. Prior to these events, the SEWG disseminates a data call, with associated criteria, for FC candidates. The FC is typically from a DHS Component and already located in the event's district whenever possible. The FC is responsible for coordinating federal support with SLTT event planners and participating federal partners. If a FC is designated, the SEWG will establish a Federal Coordination Team (FCT) to provide planning and staff support. Specific responsibilities include:

- Liaison with federal, state, and local officials
- Serve as an advisor to the Unified Coordination Group and/or incident commanders
- Resolve any federal interagency conflicts that may arise
- Consult with state and local authorities on their event security and response plans
- Ensure appropriate and coordinated Federal support is occurring in response to Federal-to-Federal, state, and local requests for assistance
- Maintain situational awareness of the event throughout the planning and execution phases
- Provide periodic updates as needed throughout the planning process to DHS

The FC does not alter or affect other federal authorities, interfere with official chains of command, or direct/replace the local incident command structure. During an incident the FC will:

- Initially coordinate federal requirements for support and assistance requested by the local Incident Commander.
- If a FEMA Joint Field Office is established, the FC will serve as an advisor to the Unified Command Group.
- Support SLTT and federal partners as appropriate until other mechanisms are in place.
- Provide situational awareness to the National Operations Center and the Secretary as requested.