

# Mississippi Incident-Specific – Terrorism Incident Annex

---

## Coordinating Agency:

MS Department of Homeland Security  
MS Dept of Public Safety

## Cooperating Agencies

Mississippi Emergency Management  
MS Dept of Public Safety  
MS Dept of Health  
MS Military Dept  
MDEQ

## Federal Coordinating Agencies

Department of Homeland Security  
Department of Justice  
Federal Bureau of Investigations

## Federal Cooperating Agencies

Department of Defense  
Department of Energy  
Department of Health and Human Services  
Department of Homeland Security  
Department of State  
Environmental Protection Agency

---

## Primary Coordinating Emergency Support Functions:

**ESF-13:** Public Safety and Security (Primary ESF)  
**ESF-10:** Hazardous Materials.  
**ESF-8:** Public Health and Medical Services  
**ESF-6:** Mass Care, Housing and Human Services  
**ESF-5:** Emergency Management  
**ESF-15:** Public Information and External Communications  
**ESF-2:** Telecommunications and Information Technology

## Introduction

### Purpose

This Annex sets forth the concept of operations for preventing responding and recovering from all threats or acts of terrorism within the State, regardless of whether they are deemed credible and/or whether they escalate to an Incident of State Significance. To accomplish this, the annex establishes a structure for a systematic, coordinated, unified, timely, and effective State response to threats or acts of terrorism within the State.

### Scope

This annex supports the Mississippi Comprehensive Emergency Management Plan and:

- Provides guidance and outlines operational concepts for the State response to a threatened or actual terrorist incident within the State; and
- Acknowledges and outlines the unique nature of each threat or incident, It addresses direction, coordination, operations for response and through out the recovery/investigation phases of an incident. Capabilities and responsibilities of the local jurisdictions, and the law enforcement and investigative activities

necessary to prevent or mitigate a specific threat or incident.

### **Policies**

The State of Mississippi regards terrorism as a potential threat to State security, as well as a violent criminal act, and applies all appropriate means to combat this danger. In doing so, the State vigorously pursues efforts to deter and preempt these crimes and to apprehend and prosecute directly, or assist other agencies in prosecuting, individuals who perpetrate or plan terrorist attacks.

To ensure the policies established in applicable Gubernatorial directives are implemented in a coordinated manner, this annex provides overall guidance to local agencies concerning the State Government's response to potential or actual terrorist threats or incidents that occur in the State, particularly those involving weapons of mass destruction (WMD), or chemical, biological, radiological, nuclear, or high-explosive (CBRNE) material.

### **Deployment/Employment Priorities**

In addition to the priorities identified in the Comprehensive Emergency Management Plan (CEMP), Response to terrorist threats or incidents within the State is based on the following priorities:

- Preserving life or minimizing risk to health; which constitutes the first priority of operations.
- Preventing a threatened act from being carried out or an existing terrorist act from being expanded or aggravated.
- Locating, accessing, rendering safe, controlling, containing, recovering, or disposing of a WMD that has not yet functioned, and disposing of CBRNE material in coordination with appropriate departments and agencies

- Apprehending and successfully prosecuting perpetrators of terrorist threats or incidents.

### **Planning Assumptions and Considerations**

In addition to the planning assumptions and considerations identified in the CEMP Base Plan, the response to terrorist threat or incident, particularly those involving WMD/CBRNE material, are based on the following assumptions and considerations:

- A terrorist threat or incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas, and may result in mass casualties.
- The suspected or actual involvement of terrorists adds a complicating dimension to incident management.
- The response to a threat or actual incident involves Local, State and Federal law enforcement to provide an investigative element to such activity.
- In the case of a threat, there may be no incident site, and no external consequences, and, therefore, there may be no need for establishment of traditional Incident Command System (ICS) elements such as an Incident Command Post (ICP) or a Joint Field Office (JFO).
- An act of terrorism, particularly an act directed against a large population center within the State involving chemical biological, nuclear, radiological, and explosive materials, will have major consequences that can overwhelm the capabilities of many local governments to respond and may seriously challenge existing State response capabilities.
- In the case of a biological attack, the effect may be temporally and geographically dispersed, with no determined or defined "incident site." Response operations may be conducted

over a multijurisdictional, multi-state region.

- A biological attack employing a contagious agent may require quarantine by State, local and Tribal health officials to contain the disease outbreak.
- If appropriate personal protective equipment and capabilities are not available and the area is contaminated with CBRNE or other hazardous materials, it is possible that response actions into a contaminated area may be delayed until the material has dissipated to a level that is safe for emergency response personnel to operate or until appropriate personal protective

equipment and capabilities arrive, whichever is sooner.

### **Situation**

The complexity, scope, and potential consequences of a terrorist threat or incident require that there be a rapid and decisive capability to resolve the situation. The resolution to an act of terrorism demands an extraordinary level of coordination of law enforcement, criminal investigation, protective activities, emergency management functions, and technical expertise across all levels of government. The incident may affect a single location or multiple locations, each of which may be an incident scene, a hazardous scene, and/or a crime scene simultaneously.

---

## **Concept of Operations**

### **Command and Control**

The Mississippi Office of Homeland Security/Department of Public Safety will serve as the lead agency for terrorist acts or terrorist threats and intelligence collection activities within the State. Investigative and intelligence activities are managed by the MSOHS/MDPS/MBI in conjunction with local effected law enforcement and the local FBI from a joint command post or Joint Operations Center (JOC). The command post or JOC coordinates the necessary assets required to respond to and resolve the threat or incident with State and local law enforcement agencies.

The lead agency will establish a forward command post to manage the threat based upon a graduated and flexible response. This command post structure generally consists of

three functional groups: Command, Operations, and Operations Support, and is designed to accommodate participation of other agencies, as appropriate.

If the threat or incident exceeds the capabilities and resources of the local, state or local FBI the additional assistance from regional and national assets to augment existing capabilities In a terrorist threat or incident that may involve a WMD or CBRNE material,

When, an actual terrorist incident has occurred, the FBI SAC becomes the Senior Federal Law Enforcement Official (SFLEO) in the. Joint operations are still conducted between Local, State and Federal Assets In this situation, the JOC Consequence Management Group is incorporated into the appropriate components of the JFO.

## **Command Group**

- Incident Command will be established at the scene of the incident and will be supported by the State Emergency Operations Center (SEOC) , The on scene Incident Command will provide command and control structure for the incident by providing leadership for the incident.
  - The Joint Information Center (JIC) Team is integrated into the IC structure when established. It is composed of the public affairs (media) officers from the participating local, State, and Federal public safety agencies. It manages information released to the public through a coordinated, unified approach The JIC provides specific guidance and expertise to the IC and SEOC and coordinates to ensure the media strategy is consistent with the overall investigative strategy.

## **Operations Group**

- The Operations Group handles all investigative, intelligence, and operational functions related to the threat, critical incident, or special event.
- Each local, state and federal unit within the Operations Group provides expertise in specific functional areas. These areas are important in the overall resolution of a incident.
- The units within the Operations Group are scalable and may be tailored to a specific threat, critical incident, or special event. Tailoring may based on equipment and expertise
- The Operations Group will consist of a Information/Intelligence unit, the Investigations unit, and Field Operations units.

## **Information/Intelligence unit**

- Information/ Intelligence unit is the central point for receiving all information and intelligence that comes into the Incident Command Post. This unit is divided into two primary sections Information and Intelligence The purpose of Information section is to ensure that telephone calls, e-mail messages, fax reports, and other incoming information are assessed for relevance to the threat, critical incident, or special event. The information is checked to determine if it has been previously reported. It is prioritized and entered into the information management system. Through this filtering mechanism the Information section ensures that only current and relevant information is disseminated to the Incident command Staff.
- The Intelligence unit manages the collection, analysis, archiving, and dissemination of relevant and valid investigative and strategic intelligence.
- The Intelligence section usually is divided into teams based on functional responsibility. Teams manage intelligence related to the crisis site or target, build intelligence portfolios.
- The Information/Intelligence Coordinator is responsible for providing guidance and direction to all personnel within the Information/Intelligence unit and coordinating the activities of the unit with all other units within the Incident. Personnel within the Information Intelligence unit are responsible for receiving incoming information, processing new information, routing follow-

up information appropriately, and implementing procedures for tracking evidentiary material that is introduced into the command post.

- The Information/Intelligence unit will maintain databases on significant elements related to the investigation (subjects, vehicles, and organizations), analyze and identify trends in activities related to the investigation (predictive and strategic intelligence), conduct liaison with outside members of the Intelligence Community, and prepare periodic briefings and reports concerning the status of the crisis or investigation. The Intelligence unit is responsible for collecting and reviewing all intelligence related to the threat, crisis, or special event to enable the State to further develop and refine strategic objectives.

### **Investigations**

- The Investigations unit provides oversight and direction to all investigative activity related to the threat, critical incident, or special event. The Investigations unit implements the strategy of the SAC by directing the collection and management of investigative information. It is composed of investigative personnel from the agencies with specific jurisdiction or authority for investigating crimes related to the threat, critical incident, or special event. The Investigations Unit Coordinator is usually Supervisory Investigator who has responsibility for investigating the most significant substantive law violation.
- Teams within the Investigations unit review all incoming information to determine investigative value. The Investigations unit assigns, tracks, and reviews all investigative leads and documents the investigation in the appropriate case file(s). The case agents or primary investigators within the Investigations unit manage all evidence and information, and prepare it for court presentation, if appropriate. The case agents or primary investigators are assisted by analytical personnel to ensure that all investigative information is pursued to its logical conclusion. A Records Check Team within the Investigations unit reviews case files and databases to ensure that all items of investigative value are identified and evaluated. The Investigations unit is responsible for collecting and reviewing all reports of investigative activity to enable the SAC to further develop and refine strategic objectives.

### **Field Operations**

- The Field Operations units are based upon the specific needs of the threat, critical incident, or special event. The personnel staffing these units are subject-matter experts in a number of specialized skill areas. Field Operations unit coordinators are responsible for ensuring the activity of the specialized units is consistent with and in support of the strategy of the Incident Command.
- Field Operations units may include representatives of tactical, negotiations, WMD/CBRNE, evidence response, surveillance, technical, or any other specialized unit deployed to the crisis site(s) or staged in readiness. The mission of these units is to provide the Incident Commander with current information and specialized assistance in dealing with the threat, critical incident, or special event. Information is communicated between the ICP and the crisis site(s) through the Field Operations unit representatives in the Incident Command Post and SEOC. This ensures that decision makers both in the SEOC and in the forward areas maintain full situational awareness. The Field Operations units coordinate their activities to ensure each is aware of the impact of their activities on the other field units.

- Local, State, and Federal law enforcement specialty units assigned to assist with field operations during the threat, incident, or special event coordinate their activities with the appropriate Field Operations units. The Joint Operations Center manages the activities of the specialized units at a strategic level. Activities at the individual or “tactical” level are managed at the crisis site(s) through forward command structures such as the Tactical Operations Center, Negotiations Operations Center, and Evidence Response Team Operations Center.

### **Operations Support Group**

- The Operations Support units designated within the JOC/SEOC ICP are based upon the specific needs of the threat, critical incident, or special event. The personnel who staff these units are subject-matter experts in a number of specialized areas. Operations Support coordinators are responsible for ensuring the activity of their units is consistent with and in support of the strategy of the Incident commander and Command Structure.
- Operations Support units can include administrative, logistics, legal, media, liaison, communications, and information management. The mission of these units is to support the investigative, intelligence, and operational functions of the Incident Command.
- A Communications unit may be established to handle radio and telephone communications to support Incident operations. The Communications unit establishes communications networks. It also establishes networks to facilitate timely and reliable information-sharing between the IC/SEOC and other command and control centers.
- The Information Technology unit is responsible for computer system operation within each unit and between units. Information technology specialists are responsible for ensuring the uninterrupted operation of the information management system used during operations.

### **The Response**

- Receipt of a terrorist threat may be through any source or medium and may be articulated or developed through intelligence sources. It is the responsibility of all Local, State, and Federal agencies and departments to notify the FBI when such a threat is received. As explained below, the FBI evaluates the credibility of the terrorist threat and notifies the HSOC, NCTC, and other departments and agencies, as appropriate.
- Upon receipt of a threat of terrorism within Mississippi, State, Local and the FBI will conduct a formal threat credibility assessment in support of operations with assistance from select interagency experts. For a WMD or CBRNE threat, this assessment includes three perspectives:
  - Technical Feasibility: An assessment of the capacity of the threatening individual or organization to obtain or produce the material at issue;
  - Operational Practicability: An assessment of the feasibility of delivering or employing the material in the manner threatened; and
  - Behavioral Resolve: A psychological assessment of the likelihood that the subject(s) will carry out the threat, including a review of any written or verbal statement by the subject(s).

- A threat assessment is conducted to determine whether the potential threat is credible, and confirm whether WMD or CBRNE materials are involved in the developing terrorist incident. Intelligence varies with each threat and impacts the level of the response. If the threat is credible, the situation requires the tailoring of response actions to use Federal resources needed to anticipate, prevent, and/or resolve the situation. The State response focuses on actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat. In addition, contingency planning focuses on the response to potential consequences and the positioning of regional resources. The threat increases in significance when the presence of a CBRNE device or WMD capable of causing a significant destructive event, prior to actual injury or loss, is confirmed or when intelligence and circumstances indicate a high probability that a device exists. In this case, the threat has developed into a WMD or CBRNE terrorist situation requiring an immediate process to identify, acquire, and plan the use of State resources to augment local authorities in lessening or averting the potential consequence of terrorist use or employment of WMD or CBRNE material. It should be noted that a threat assessment would also be conducted if an incident occurs without warning. In this case, the assessment is focused on criminal intent, the extent of the threat, and the likelihood of secondary devices or locations.
- The FBI manages a Terrorist Threat Warning System to ensure that vital information regarding terrorism reaches those in the U.S. counterterrorism and law enforcement community responsible for countering terrorist threats. This information is coordinated with MOHS.
- The FBI leads the criminal investigation related to an actual confirmed terrorism incident, and the State Fusion Center (MOSAIC) along with the Strategic Information and Operations Center (SIOC) is the focal points for all intelligence related to the investigative law enforcement response to the incident. Consistent with the state CEMP and the Federal NRP, affected State and Federal agencies operate emergency operations centers, as necessary. State and Federal Law Enforcement initiates' appropriate liaison with other State and Federal agencies to activate their operations centers and provide liaison officers.
- . The Incident Commander establishes initial operational priorities based upon the specific circumstances of the threat or incident. This information is then forwarded to State and Federal Emergency Operations Centers to coordinate identification and deployment of appropriate resources.
- Once a terrorism incident is confirmed a JOC is established by the FBI under the operational control of the FBI SAC, and acts as the focal point for the field coordination of criminal investigation, law enforcement, and intelligence activities related to the threat or incident. When a Principal Federal Official (PFO) is designated for a terrorism incident, the FBI SAC provides full and prompt cooperation, resources, and support to the PFO, as appropriate and consistent with applicable authorities. The PFO (or an initial PFO designated by the Secretary of Homeland Security) may elect to use the JOC as an initial operating facility for strategic management and identification of State, local, and Tribal requirements and priorities, and coordination of the Federal response. The FBI SAC coordinates with the PFO, including providing incident information to the PFO as requested, coordinating the public communications strategy with the PFO, and approving Federal interagency communications for release to the public through the PFO. It is recognized, however, that in some cases it may be necessary for the FBI SAC to respond directly to media/public inquiries on investigative operations and matters affecting law enforcement operations, particularly during the early stages of the emergency response.

- The local FBI Field Office activates a Crisis Management Team to establish the JOC in the affected area, possibly collocated with an existing emergency operations facility. In locating the JOC, consideration is given to the possibility that the facility may have to accommodate other Federal incident management field activities including the JFO, the JIC, and other supporting teams. Additionally, the JOC is augmented by outside agencies, including representatives from the DEST (if deployed), who provide interagency technical expertise as well as interagency continuity during the transition from an FBI command post structure to the JOC structure.
- Based upon a credible threat assessment and a request by the SAC, the FBI Director and DHS Under Secretary for Emergency Preparedness and Response, in consultation with the Attorney General and Secretary of Homeland Security, may request authorization through the National Security Council to deploy the Disaster Emergency Services Team (DEST) to assist in mitigating the crisis situation. The DEST is a rapidly deployable, interagency team responsible for providing expert advice and support concerning the Federal Government's capabilities in resolving the terrorist threat or incident. This includes law enforcement, criminal investigation, and emergency management assistance, technical and scientific advice, and contingency planning guidance tailored to situations involving chemical, biological, or nuclear/radiological weapons.
- Upon arrival at the FBI command post or JOC, the DEST may act as a stand-alone advisory team to the SAC providing recommended courses of action. Although it would be unusual, the DEST may be tasked to deploy before a JOC is established. The DEST may handle some of the specialized interagency functions of the JOC until the JOC is fully staffed. The DEST emergency management component merges into the Consequence Management Group in the JOC structure.
- Prior to an actual WMD or CBRNE incident, law enforcement, intelligence, and investigative activities generally have priority. When an incident results in the use of WMD or CBRNE material, rescue and life-safety activities generally have priority. Activities may overlap and/or run concurrently during the incident management, and are dependent on the threat and/or the strategies for responding to the incident.
- Upon determination that applicable law enforcement/intelligence goals and objectives are met and no further immediate threat exists, the FBI SAC may deactivate the JOC and order a return to routine law enforcement/investigative operations in accordance with pre-event protocols.
- When an incident occurs and an ICP is established on-scene, FBI personnel integrate into the ICP to enhance the ability to carry out mission. Three specific positions within an ICP are provided. The first FBI Special Agent (SA) or Joint Terrorism Task Force (JTTF) member responding receives an initial briefing from the Incident Commander or his/her designee and works closely with the Incident Commander as a member of the Unified Command. The FBI representative then informs the local Field Office of the current situation and, if necessary, requests additional assets. When a more senior FBI SA arrives on the scene, he/she assumes the role of the FBI representative in the Unified Command.
- When an incident occurs and an ICP is established on-scene, MSOHS personnel integrate into the ICP to assist with their deployment of State assets equipped and trained to assist with a Terrorism Incident. DPS/MSOHS receives an initial briefing from the Incident Commander or his/her designee and works closely with the Incident Commander as a member of the Unified Command. The DPS/MSOHS representative then informs the SEOC and the Director

of MS Office of Homeland Security of the current situation and, if necessary, requests additional assets.

Note: Operational control of assets at the scene is retained by the designated officials representing the agency (local, State, or Federal) providing the assets.