KING COUNTY, WASHINGTON
EMERGENCY MANAGEMENT PLAN
TERRORISM INCIDENT, LAW ENFORCEMENT & INVESTIGATION ANNEX

THIS DOCUMENT IS A PLAN FOR RESPONDING TO A TERRORIST-RELATED SITUATION OR INCIDENT, OR FOR DEPLOYING PERSONNEL IN SUCH A SITUATION.

PORTIONS OF THIS DOCUMENT MAY BE EXEMPT FROM PUBLIC DISCLOSURE PURSUANT TO RCW 42.56.420. REQUESTS FOR PUBLIC DISCLOSURE OF THIS DOCUMENT, OR PARTS THEREOF, SHOULD BE REFERRED IMMEDIATELY TO THE KING COUNTY PROSECUTING ATTORNEY’S OFFICE.

DISTRIBUTION OF THIS DOCUMENT BEYOND THE INTENDED PARTY IS PROHIBITED UNLESS AUTHORIZED IN WRITING IN ADVANCE BY THE KING COUNTY PROSECUTING ATTORNEY’S OFFICE OR DESIGNEE.
I. INTRODUCTION

A. Purpose

The purpose of the King County Terrorism Incident, Law Enforcement & Investigation Annex (TIA) is to establish a framework for responding to and recovering from a terrorist-initiated incident to include weapons of mass destruction (WMD). To accomplish this, the annex establishes a structure for systematic coordination, unified, timely and effective county response to threats or acts of terrorism within the county.

B. Scope

This annex supports the King County Comprehensive Emergency Management Plan (CEMP) and:

- Provides guidance and outlines operational concepts for the county response to a threatened or actual terrorist incident within the county.
- Acknowledges and outlines the unique nature of each threat or incident. This annex addresses direction, coordination, operations for response as well as throughout the recovery/investigation phases of an incident.
• Outlines the capabilities and responsibilities of the all local, State, and Federal jurisdictions, and the law enforcement and investigative activities necessary to prevent or mitigate a specific threat or incident.

This Annex addresses the jurisdictions the King County Sheriff’s Office provides law enforcement services including unincorporated and contract agencies. Although this Annex is incident specific, any number of Emergency Support Functions or Appendices may be necessary to the response.

II. POLICIES & PLANS

This Terrorism Incident Annex is developed, promulgated, and maintained pursuant to local, state and federal statutes and regulations. King County regards terrorism as a potential threat to the community, as well as violent criminal act, and applies all appropriate means to combat this danger. In doing so, the county vigorously pursues efforts to deter and preempt these crimes and to apprehend and prosecute directly, or assist other governments in prosecuting, individuals who perpetrate or plan terrorist attacks.

• Local
  ▪ Interlocal Agreement for Joint Participation in Homeland Security and Emergency Preparedness Programs (Tri-County Agreement between King, Pierce and Snohomish Counties)
  ▪ King County Homeland Security Policy Motion #11728
  ▪ Individual emergency and terrorism plans for King County cities, special purpose districts, public and private organizations (Not Subject to Public Disclosure)
  ▪ Regional Hazard Mitigation Plan for King County
  ▪ Terrorism Threat Notification Protocol-King County Sheriff and King County Executive

• State
  ▪ State Fire Mobilization Plan (http://emd.wa.gov/)
  ▪ State Law Enforcement Mobilization Plan (in development)

• Federal
  ▪ Homeland Security Presidential Directives (HSPD) http://www.whitehouse.gov/
  ▪ Presidential Policy Directive (PPD) – 25 – The Federal Bureau of Investigation acting primarily through the Joint Terrorism Task Force (JTTF), has the lead responsibility for investigative activities involving Federal crimes of terrorism. This includes the receipt and resolution of suspicious activities or acts in preparation of terrorist activities.
  ▪ PDD-62 Protection Against Unconventional Threats to Homeland and Americans Overseas http://www.fas.org/
III. 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.

Types of terrorism include cyber terrorism (communications and information systems), agro terrorism (food supplies) and the use of weapons of mass destruction (WMD). Weapons of mass destruction include chemical, biological, radiological, nuclear and explosive (CBRNE) weapons that can affect people, property and infrastructure locally, regionally or worldwide. The nature of such weapons makes mitigation, response and recovery issues difficult. King County’s proximity to waterways, interstate highways and the Canadian border increase its vulnerability.

There are potential vulnerable sites in King County that are so vital to the region and Nation that their incapacity or destruction would have a debilitating impact on security, economic security, and/or public health and safety.

Potential terrorism scenarios remain difficult to predict, prepare for and defend against. An all-hazards approach for emergency management planning provides a single standardized and integrated system, which can also be applied to terrorist attacks that can potentially take many forms. Jurisdictions and agencies within King County periodically perform threat and vulnerability assessments and hazard identification and vulnerability assessments.

There are three types of possible terrorist response scenarios to credible threats, pre-planned and special events, non-specific threats, and no-notice. Pre-planned and special events scenario provides advance notification and allows for planning, coordinating, pre-staging of assets, rehearsing, and conducting joint operations exercises. Local, state and federal assets should be
pre-deployed and ready to react to any contingency. Unified command should already be in place.

For a Non-specific threat scenario an articulated threat immediately initiates the FBI threat assessment process to determine if the threat is credible or a hoax. If the threat is credible, the FBI notifies local, state and federal authorities for appropriate response actions. This scenario may or may not provide adequate time for preparation or pre-deployment of local, state and federal response assets.

During a No-notice scenario the local first responder community is the first to arrive on site. The Incident Command System (ICS) should be established in accordance with local policies. Local and state authorities should request federal assistance in accordance with established emergency operations plans. The Incident Commander transitions from a single to a unified command to include the FBI.

A. Planning Assumptions

In addition to the planning assumptions and considerations identified in the CEMP Basic 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, without a determined or defined “incident site.” Response operations may be conducted over a multi-jurisdictional, 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 (PPE) 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.
The sharing of information is vital during a threat of terrorism in the region. The Sheriff’s Office may possess information of a classified nature that cannot be immediately shared with other departments and agencies to include the Executives office until they receive permission to do so.

Relative and corroborated information is passed on to the Sheriff on a right-to-know/need-to-know basis. The Sheriff may also receive information directly from federal, state, and local agencies.

Depending on the situation, economic consequence management and recovery will be addressed by local, state, and federal authorities in coordination with the private sector.

Depending upon the situation, a unified command may be established between law enforcement, fire/EMS agencies, Public Health-Seattle & King County, hospitals, and public works depending on the nature of the terrorist incident.

Local Emergency Operations Centers (EOCs) may be activated in support of their jurisdictions, agencies and organizations.

There is no guarantee implied by this Annex that a perfect response to a terrorism incident involving weapons of mass destruction will be practical or possible.

B. Accessibility of Terrorism Information

Consideration should be given to maintaining, in a secure place, information critical to a jurisdiction, tribe, organization or agencies’ response to a terrorist incident. Threat assessment information, plans, procedures, and other documents, information and resources related to terrorism preparedness and response may provide useful information to terrorists. This information may aid terrorists in the planning and execution of criminal or terrorist acts.

RCW 42.56.420 exempts the following class of information from public records disclosure:

(1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and
(b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism;

(2) Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility or any individual’s safety;

(3) Information compiled by school districts or schools in the development of their
comprehensive safe school plans under RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school;

(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities; and

(5) The *security section of transportation system safety and security program plans required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180.

IV. CONCEPT OF OPERATIONS

The King County Sheriff’s Office will serve as the lead local agency for terrorist acts or terrorist threats and intelligence collection activities within unincorporated King County and the contract agencies served.

When, an actual terrorist incident has occurred, the FBI Special Agent in Charge (SAC) becomes the Senior Federal Law Enforcement Official (SFLEO). 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.

Investigative and intelligence activities are managed by the King County Regional Criminal Intelligence Group (KCRCIG) in conjunction with the Washington State Fusion Center and the local Federal Bureau of Investigations (FBI) from an Incident Command Post (ICP) or Joint Operations Center (JOC). The ICP or JOC coordinates the necessary resources required to respond to and resolve the threat or incident with local law enforcement agencies.

If the terrorist threat or incident which has involved a WMD or CBRNE material exceeds the capabilities and resources of the state, local, tribal and/or local FBI, additional assistance from regional and national assets will be requested to augment existing capabilities. State and local governments exercise primary authority to respond to the consequences of terrorism; the federal government provides assistance as required. Consequence management is generally a multifunction response.

A. Command

Incident Command (IC) will be established at the scene of the incident and will be supported by the King County Emergency Coordination Center (ECC). The on-scene IC will provide command and control structure for the incident by providing leadership for the incident at the incident site.

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 ECC.

B. Operations Section

The Operations Section 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 an incident.

The units within the Operations Section are scalable and may be tailored to a specific threat, critical incident, or special event. Tailoring may be based on equipment and expertise.

The Operations Section will consist of an Information/Intelligence unit, an Investigations unit, and a Field Operations unit(s).

1. Information/Intelligence Group

The Sheriff’s Office Regional Criminal Intelligence Group may liaison with the FBI Joint Terrorism Task Force (JTTF) and other intelligence and information gathering groups or may choose to create an Information/Intelligence Group. The Information/Intelligence Group is the central point for receiving all information and intelligence that comes into the Incident Command Post. This Group will consist of intelligence analysts from the KCCCRIG and the FBI - Seattle Field Office in a joint effort between the FBI and the county. The Intelligence Group is divided into two primary units Information and Intelligence.

The purpose of the Information Unit 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 an information management system. Through this filtering mechanism the Information Unit 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 Unit usually is divided into teams based on functional responsibility. Teams manage intelligence related to the crisis site or target and build intelligence portfolios.

The Information/Intelligence Supervisor is responsible for providing guidance and direction to all personnel within the Information/Intelligence Group and coordinating the activities of the units with all other Groups within the Incident. Personnel within the Information/Intelligence Group 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 Group 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.

2. Investigations Group

The Investigations Group provides oversight and direction to all investigative activity related to the threat, critical incident, or special event. The Investigations Group implements the strategy of the FBI Special Agent in Charge (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 Group Supervisor is usually a supervisory investigator who has responsibility for investigating the most significant substantive law violation.

Teams within the Investigations Group review all incoming information to determine investigative value. The Investigations Group 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 Group 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 Group is responsible for collecting and reviewing all reports of investigative activity to enable the SAC to further develop and refine strategic objectives.

3. Operational Groups

The Operational Groups 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. Group Supervisors are responsible for ensuring the activity of the specialized units is consistent with and in support of the strategy of the Incident Command.

Operational Groups 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 groups is to provide the Incident...
Commander with current information and specialized assistance in dealing with the threat, critical incident, or special event.

Information may be communicated between the ICP and the crisis site(s) through the Group representatives in the Incident Command Post. This ensures that Incident Commanders and other supervisors maintain full situational awareness. The groups 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 operations during the threat, incident, or special event coordinate their activities with the appropriate groups. 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.

4. Support Units

The Support Units are designated within the ICP/JOC 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. Unit Leaders 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.

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 ICP/JOC/ECC 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.

V. 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 Homeland Security
Operations Center (HSOC), National Counter Terrorism Center (NCTC), and other departments and agencies, as appropriate.

Upon receipt of a threat of terrorism within King County; state, local and tribal, and federal agencies along with 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 county 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 the JTTF, Washington State Fusion Center and KCRCIG.

The FBI leads the criminal investigation related to an actual confirmed terrorism incident, and the FBI – JTTF along with the Washington State Fusion Center and the Strategic Information and Operations Center (SIOC) are the focal points for all intelligence related to the investigative law enforcement response to the incident. Consistent with the ECC, local EOCs, state CEMP and the Federal NRF, affected state and federal agencies operate emergency operations centers, as
necessary. Local enforcement initiates’ appropriate liaison with other state and federal agencies to activate their operations centers and provide liaison officers.

The Incident Commander (IC) establishes initial operational priorities based upon the specific circumstances of the threat or incident. This information is then forwarded to ECC, 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, with assistance from the local jurisdictions and will act 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 FBI Seattle 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 a Disaster Emergency Support Team (DEST) (if deployed), who provide interagency technical expertise as well as interagency continuity during the transition from an Incident Command Post 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 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 Incident Command Post or JOC, the ERT 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 existing Incident Command Structure (ICS) 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. Multiple activities and agency’s duties 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 abilities of the state and local agencies 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 the King County Sheriff’s Office personnel will respond and establish an ICP on-scene. Outside agency personnel may respond and integrate into the ICP to assist with the deployment of assets equipped and trained to assist with a Terrorism Incident. All agency representatives will receive an initial briefing from the Incident Commander or their designee and will coordinate with the Incident Commander as a member of the Unified Command. The Incident Commander or their designee informs the Command Duty Officer of the current situation and, if necessary, requests additional assets. The Command Duty Officer informs the Office of Emergency Management Duty Office of the current situation and, if necessary, requests additional assets. Emergency management representatives from affected jurisdictions and emergency responder organizations may respond to the JOC to support the Command. Such coordination between local decision makers and the JOC Command may also be take place by video conferencing.

Mass care and sheltering may be managed as designated in the King County Comprehensive Emergency Management Plan (CEMP), ESF 6, Mass Care, Emergency Assistance, Housing and Human Services. Shelter-in-Place procedures are covered in the CEMP, ESF 10, Oil and Hazardous Materials, Isolation & Evacuation section or in the King County Local Emergency Planning Committee (LEPC) Hazardous Materials Plan.

Mass casualty management, including triage, treatment and transportation, will follow the procedures established in the Seattle-King County Mass Casualty Incident (MCI) Plan. Additional planning guidance is provided in the King County CEMP, ESF 8, Public Health and Medical Services.
Fatality management, including incident scene preservation and incident/scene investigation, reconstruction and the prevention of the commingling of remains shall follow the procedures of the King County Medical Examiner. Additional guidance is provided in the Seattle-King County MCI Plan.

When an incident requires the deployment of the National Asset Response Unit (NARU) to assist with WMD terrorism incidents the state will assist FBI- Seattle Division in supporting the NARU deployment and convoy operations.

Operational control of assets at the scene is retained by the designated officials representing the agency (local, state, or federal) providing the assets.

Actual procedures are deemed sensitive security information based on their detailed account of field operating procedures, detection and identification methods.

VI. RESPONSIBILITIES

In the event of a terrorist response, the Federal government activates the National Response Framework - Terrorism Annex. Presidential Decision Directive-39 identifies lead agency responsibility to manage and coordinate a specific function—either crisis management or consequence management on the basis of having the most authorities, resources, capabilities, or expertise relative to accomplishment of the specific function.

Responsibilities listed are specifically related to terrorist or WMD incidents. All general information can be found in the King County Emergency Management Plan, Basic Plan, Section V. Responsibilities, or in specific Emergency Support Functions (ESF).

A. Primary Agency

The following agency has the core local response to incidents of terrorism:

**King County Sheriff’s Office (KCSO):**
- Maintain law and order by activating the King County Emergency Management Plan, ESF 13-Public Safety and Security.
- Activate the KCSO Critical Incident Management Plan that includes incident-specific procedures for hazardous materials and terrorism incidents.
- Assess and adjust the KCSO Operational Readiness Level (four-tiered system) in order to protect infrastructure from external attack and enhance response readiness posture by increasing staffing and curtailing non-critical functions.
- May provide information to the King County Executive using the established “Terrorism Threat Notification Protocol-King County Sheriff and King County Executive.”
- The KCSO Special Operations Division will coordinate with the King County Office of Emergency Management as referenced in the “Terrorism Threat Notification Protocol-King County Sheriff and King County Executive.”
- Provide regional services as needed to include air, marine and surface support.
• Provide liaisons to the JTTF and the JOC.
• Contact the FBI if incident is a confirmed or highly credible threat.
• Contact Public Health-Seattle & King County for evaluation of potential bio-terrorism incidents.
• Contact Public Health-Seattle & King County for access to sample evaluation of suspect Bioterrorism samples by the State Health Lab.
• Upon request from Public Health-Seattle & King County may assist with sample transportation if appropriate and staff is available.

B. Support Agencies

The following agencies and organizations provide supporting response to incidents of terrorism:

**King County Office of Emergency Management:**
• Has responsibility for even broader areas concerning the public safety in regards to consequence management and the continuity of public services.
• Activate the King County ECC in support to jurisdictions, organizations or agencies, or may act as the coordination point for participating local, state and federal agencies during ongoing response and recovery activities for any terrorism incident - physical, cyber or other.
• If requested, use the Regional Disaster Plan for Public & Private Organizations and Regional Terrorism Incident Annex.
• Seek to integrate crises and consequence management functions in King County government, and coordinate with state, federal and regional partners as appropriate.

**Public Health-Seattle & King County:**
• The Department of Public Health – Seattle & King County will be the lead consequence management agency for bio-terrorism.
• Activate the Region 6 (King County) Regional Hospital Plan-Preparedness & Response for Bio-Terrorism.
• Provide assessments of the public health impacts of WMD incidents and seek assistance from the WA State Department of Health if needed.
• Activate the Public Health-Seattle & King County Emergency Response Plan and appropriate CBRNE Annex.
• If needed, activate the Bioterrorism Mass Vaccination/Distribution Emergency Operations Plan.
• Direct the provision of immunizations, prophylaxis, and other preventative treatment.
• Coordinate with the State Department of Health for the delivery and distribution of the Strategic National Stockpile.
• Exercise oversight and direction of all environmental health issues related to a terrorist incident.
• Authorize testing at the State Lab of suspected bio-terrorism samples from a credible threat incident.
• Contact dispatch, Public Health-Seattle & King County and/or Hospital Control if a victim may be contaminated, has symptoms resembling terrorist weapon material exposure or medics have been impacted.
- Notify hospitals of suspected or anticipated health effects of a CBRNE incident.
- Notify local responders, emergency management and municipalities of State Lab identification of agents.

**King County Department of Information & Resource Management (KCIT):**
- For cyber-related threats or incidents, OIRM will coordinate closely with City of Seattle, Washington State, and others to investigate cyber terrorist activities as they are emerging, to classify them as to type, priority, and severity and to mobilize an appropriate response.
- OIRM has internal, specialized resources to deal with e-mail viruses, web applications, and network issues.
- OIRM will coordinate response with the City of Seattle due to reliance on shared resources and service providers.
- OIRM will draw upon other King County resources (e.g. LAN administrators) as dictated by the incident and response.

**Local Law Enforcement other than KCSO:**
- Local law enforcement will use their agency’s terrorism response protocols, policies and procedures, emergency response plans and Emergency Support Function (ESF) 13-Public Safety and Security.
- If required or needed, local law enforcement may provide security and maintain order at decontamination sites, field and area hospitals, functional areas, and command post.
- Depending upon availability of sworn personnel, law enforcement may be called upon to assist with the enforcement of a quarantine order or to provide security at hospitals.
- Provide assistance if needed to the Joint Terrorism Task Force (JTTF) and liaisons to the FBI Joint Operations Center (JOC).
- Mutual aid request from local law enforcement will typically be requested directly with other agencies.

**Local Fire Agencies:**
- Health and medical services responsibilities for Fire agencies are currently included in the King County Emergency Management Plan, ESF 8 Public Health and Medical Services.
- Fire Agencies will use their agency’s terrorism response protocols, policies and procedures, emergency response plans and Emergency Support Function, ESF 4-Firefighting. Local fire agencies in coordination with the King County Sheriff’s Office will manage operations of Hazardous Materials (HAZMAT) Response Teams as per Hazardous Materials Response Plans and ESF 10-Oil and Hazardous Materials.
- Local, county, and regional fire mobilization assets and technical rescue resources are coordinated for King County through the Regional Fire Resource Coordinator as listed in the King County Fire Resource Plan and the South Puget Sound Region Fire Resource Mobilization Plan.
- Contact the Department of Public Health-Seattle & King County when a bio-terrorist incident is suspected.
- Request dispatch notification of local law enforcement and/or the FBI when necessary.
Local Hospitals:
- Activate the Region 6 (King County) Regional Hospital Plan-Preparedness & Response for Bio-Terrorism.
- Provide support for the King County Emergency Management Plan, ESF 8 Public Health and Medical Services and the Regional Disaster Plan.

American Red Cross (ARC):
- Provide support for the King County Emergency Management Plan, ESF 8 Health/Human Services and the Regional Disaster Plan, ESF 8 – Health and Medical Services.
- Activate the ARC of King-Kitsap Counties Weapons of Mass Destruction/Terrorism Annex to Chapter Disaster Response Plan.
- Provide mass care support at decontamination shelters.

Puget Sound Clean Air Agency (PSCAA):
- PSCAA operates the BioWatch Air Monitoring Program and provides samples to the State Department of Health Laboratory for analysis.
- In support of debris management, PSCAA can measure ambient air concentrations for fine particulate materials and be a liaison for determining additional needed air monitoring services.
- Work in coordination with the state and local health department in operation of the BioWatch Air Monitoring Program.

Port of Seattle (POS):
- The Port of Seattle (POS) is a signatory to the Regional Disaster Plan and has resources that, if available and applicable, could be used to assist response and recovery to a terrorism incident.
- The POS airport and Seaport primary objective is to continue to serve regional needs by maintaining normal operational levels until conditions warrant otherwise.
- POS Police and Fire will respond with mutual aid when and as available.
- Upon notification of a confirmed or verified suspected terrorist incident, the POS will immediately activate, and staff as necessary the Port of Seattle Emergency Command Center to serve as the Port’s initial secured communications and coordination center.
- Establish and maintain electronic communications if available, or use other available communication modes if needed, to receive intelligence and operational updates.
- Prepare to execute standard requirements of the Transportation Security Agency (TSA) in accordance with elevated threat levels and communicate the effects of such requirements on air and marine operations to the King County RCECC and affected jurisdiction(s).
- As resources permit and depending on the incident location, send a Liaison to the King County ECC or Seattle EOC if needed for coordination and communication to respond and recover from a terrorism incident.
- Prepare the airport Mobile Command Post for possible deployment to waterfront areas as needed and if available.
- Send a representative to participate in the Joint Information Center (JIC) as needed or Joint Operational Center (JOC) as ordered.
- Conduct internal briefings and actions as required to keep passengers, airlines, tenants, government agencies and Port departments abreast of incidents and operational requirements.

**Washington State Emergency Management Division (WAEMD):**
- The Washington Emergency Management Division has developed a Washington State Comprehensive Emergency Management Plan, Annex A – Terrorism (not subject to public disclosure). The document outlines the core state responsibilities and resources involving incidents of terrorism. In the event of a terrorism incident in Washington State, the WAEMD will activate the WAEMD EOC. In the event of a chemical or radiological incident, the WAEMD can activate the “Integrated Fixed Facility Radiological And Chemical Protection Plan. Annex B, Appendix 1 of this Plan provides U.S. Department of Energy emergency response assets and response times that are available by request through the Washington State Emergency Management Division. The WAEMD will also alert and notify jurisdictions, states and Canada of an incident, and coordinate resources.

**Washington State Departments:**
- Many Washington State departments will support local response and recovery efforts from a terrorist incident. The WAEMD is the state coordinating agency for requesting state assistance. Other state departments that may assist if needed include, but are not limited to:
  - State Patrol
  - The Military Department – National Guard for providing military resources, which may include both equipment and personnel to aid in the response to a terrorist incident, including the 10th Civil Support Detachment (CSD) WMD.
  - State Department of Health for providing laboratory services and assessments of the public health impact of terrorist incidents, coordinating the reception and deployment of federal and out-of-state health resources supporting the terrorist incident response and recovery, and providing support to local health agencies.
  - State Department of Agriculture for monitoring food, feed and other commodities for contamination and ensure that products distributed for consumption are safe, and work with local health agencies to provide information to the public regarding food and product safety.
  - State Department of Transportation for coordinating activation of needed WSDOT personnel and equipment. In the event of a terrorist incident, the Washington State Ferry system falls under the purview of the U.S. Coast Guard and will follow appropriate MARSEC level responses as determined by the Captain of the Port.
  - State Department of Information Services for the dissemination of information related to cyber activities and to assist with response scenarios.
  - Other State Departments as needed.

**Department of Homeland Security/Federal Emergency Management Agency:**
- The Department of Homeland Security (DHS) provides direction for the application of federal government resources used to support domestic counter terrorism operations. The DHS gathers information related to domestic counter terrorism preparedness, response, and recovery, and provides information to the public, the private sector, local and State authorities, federal departments and agencies, and the President.
• The Attorney General, generally acting through the FBI as Primary Federal Agency (PFA) for the domestic counter terrorism functional area, is responsible for coordinating domestic intelligence collection activities, coordinating activities of the law enforcement community to detect, prevent, preempt, or disrupt terrorist attacks, conducting the criminal investigation of terrorist threats or acts, and identifying the perpetrators and bringing them to justice.

• Under Presidential Directive Decision #39-US Policy on Counter Terrorism, the Federal Emergency Management Agency (FEMA) supports the FBI LFA as the lead agency for consequence management until the overall LFA role is transferred to FEMA. FEMA will consult with the Governor’s office and the White House to determine if a Federal consequence management response is required and if FEMA is directed to use Stafford Act authorities. This process involves appropriate notification and coordination with the FBI, as the overall Lead Federal Agency (LFA).

• FEMA will appoint a Regional Operations Center (ROC) Director or Federal Coordinating Officer (FCO) to manage and coordinate the federal consequence management response in support of State and local governments. In coordination with the FBI, the ROC Director or FCO will convene meetings with decision makers of federal, state, and local emergency management and technical support agencies, as appropriate, to formulate incident action plans, define priorities, review status, resolve conflicts, identify issues that require decisions from higher authorities, and evaluate the need for additional resources.

Federal Bureau of Investigation (FBI):

• Under Presidential Policy Directive (PPD) – 25, the Federal Bureau of Investigation acting primarily through the Joint Terrorism Task Force (JTTF), has the lead responsibility for investigative activities involving Federal crimes of terrorism. This includes the receipt and resolution of suspicious activities or acts in preparation of terrorist activities.

• Under PDD-39, The FBI is the crisis management Lead Federal Agency (LFA) responsible for the criminal investigation, crime scene, and apprehension of those responsible for terrorist incidents, threats and suspected terrorist incidents and designates appropriate liaison and advisory personnel to support the JOC, EOC and the local ICS infrastructure.

• Whenever federal consequence management is required, the local FBI command post expands into a Joint Operations Center (JOC).

• The FBI determines when a threat of terrorism warrants consultation with the White House through the Attorney General.

• The FBI works with the Department of Homeland Security to establish and operate a Joint Information Center (JIC) in the field as the focal point for information to the public and the media concerning the federal response to the emergency.

• If needed, the FBI deploys interagency support teams and resources to ensure that the full range of necessary expertise and capabilities are available to the on-scene coordinator.

United States Coast Guard:

• The U.S. Coast Guard serves as (1) the lead federal agency (LFA) for Maritime Homeland Security when responses require civil authorities; (2) the Federal Maritime Security Coordinator in U.S. ports as designated by the Maritime Transportation Security Act of 2002; (3) a supporting agency to the Federal Emergency Management Agency for declared disasters or emergencies under the Federal Response Plan; (4) a supporting agency to the
LFA for specific incidents under the provisions of the current *U.S. Government Interagency Domestic Terrorism Concept of Operations Plan* and its projected replacement by the *Federal Incident Management Plan*; and (5) as a supporting or supported commander for military operations conducted under Title 10.

- The Captain of the Port Puget Sound is the pre-designated Coast Guard Incident Commander (CGIC) for a WMD or terrorist incident in the Puget Sound area. The CGIC will represent the Coast Guard in any ICS organization formed for a multi-agency response and will exercise command and control authority over all Coast Guard resources assigned to an incident when activated for contingency response.

**Other Federal Agencies:**
- In accordance with federal directives and if needed, appropriate federal agencies will activate technical operations capabilities to support federal response to threats or acts of WMD terrorism. Assistance could include threat assessment, consultation, agent identification, hazard detection and reduction, environmental monitoring, decontamination, and long-term site restoration (environmental cleanup) operations, DEST deployment, technical advice, operational support, tactical operations, support for civil disturbance, and custody, transportation, and disposal of a WMD device. Federal agencies could include the Departments of Energy, Defense, Health and Human Services, Environmental Protection Agency, and others as needed.

**VII. RESOURCE REQUIREMENTS**

Resource logistics and support are outlined in the King County Emergency Management Plan, ESF 7, Resource Support and through the Regional Disaster Plan for Public and Private Organizations that includes the Omnibus Mutual Aid Agreement. Additional resources are available from the Washington State Emergency Management Division and the Federal Department of Homeland Security. Listings of resources are available in:

- Washington State Comprehensive Emergency Management Plan, Annex A - Terrorism (not subject to public disclosure)
- Washington State Fire Mobilization Plan
- Washington State Integrated Fixed Facility Radiological And Chemical Protection Plan

**VIII. REFERENCES**

- King County Emergency Management Plan (KCEMP)  
- Region 6 (King County) Regional Hospital Plan-Preparedness & Response for Bio-Terrorism Plan
- Seattle-King County Mass Casualty Incident Plan (MCI)  
  Regional Hazard Mitigation Plan and Hazard Identification Vulnerability Analysis (HIVA) for King County
- Washington State Comprehensive Emergency Management Plan, Annex A, Terrorism (Not subject to public disclosure)
IX. TERMS AND DEFINITIONS

See Appendix 1, Definitions and Appendix 2, Acronyms