

*Jefferson County, Alabama
Comprehensive Emergency Management Plan*

Section 6: D

**Civil Disturbance / Terrorism
(Domestic Preparedness)**

Preface

In the wake of the World Trade Center Bombing in New York and the Oklahoma City Bombing, terrorism has become an increasing concern for emergency management, emergency responders, and the public at large.

Terrorism is the threat or use of force or violence against persons and property to achieve political / social ends and is usually associated with community disruption and / or multiple injuries or death.

This plan augments the existing Jefferson County Comprehensive Emergency Management Plan.

I. PURPOSE

To provide general guidance for the coordination of emergency operations and resources within the county to save lives, protect property and restore order in the event of a civil disturbance or terrorism event.

II. SCOPE

A. Antiterrorism

Antiterrorism involves the measures taken by installations, organizations or individuals to reduce the probability of their becoming a victim of terrorism. Educational programs, physical security, personal protection techniques, and operational patterns are all passive means of making potential targets less appealing to terrorists.

Vital components of an antiterrorism program include: information and intelligence gathering, development and implementation of preventative measures, in-depth planning, and specialized training.

B. Counterterrorism

Counterterrorism is the full range of offensive measures to prevent, deter and respond to terrorism. This includes direct contact with the terrorist force or its representative to end the incident with minimum disruption or loss of life and property. Participation in counterterrorism actions is generally limited to those forces with special training and expertise. This begins participation by "crisis" and "consequence" management actions.

C. Crisis Management

Crisis Management is the law enforcement response to the causes of terrorist incidents, terrorists, and their weapons. It includes measures to identify, acquire, and plan the use of resources needed to anticipate, isolate, prevent, and/or resolve a threat or act of terrorism.

The federal government exercises preeminent authority and responsibility in crisis management. The federal crisis management effort is led by the Federal Bureau of Investigation (FBI) with assistance from other federal, state, and local agencies as necessary.

D. Consequence Management

Consequence management addresses the consequences of terrorism, the effects upon people, their property, and their communities. It includes measures to protect public health and safety, restore essential government services, and provide emergency relief to government, businesses, and individuals affected by the consequences of terrorism.

The State of Alabama and local agencies exercise preeminent authority to make decisions regarding the consequences of terrorism. This authority would normally rest with the incident commander and local emergency services organization. The federal government provides assistance as required. The Federal Emergency Management Agency (FEMA) coordinates federal agencies consequence management support with the State of Alabama.

III. SITUATION AND ASSUMPTIONS

Jefferson County's response to a terrorist incident will be determined by the material involved (i.e., firearms, explosive, nuclear, incendiary, biological, or chemical) and by the authorities, plans and operations that are triggered.

A. Situation

1. A civil disturbance/terrorism emergency situation could occur at any time and with a minimum of warning.
2. Law Enforcement is responsible for preserving the peace and suppression of any civil disturbances/terrorism, including demonstrations and unlawful acts ranging from passive disobedience to mass insurrection.
3. In a terrorist incident, the area of operations is potentially a crime scene, a hazardous materials site and a disaster area -- spanning the borders of several local jurisdictions. In order to organize a complex on-scene operation, operational boundaries need to be defined with common terminology and procedures for officials responding to the crime, the hazardous materials incident, and the disaster. Operational boundaries may be used to control access to the area, target public information messages, assign operational sectors among responding organizations, and assess potential impacts on the population and the environment. The physical location of these boundaries will depend on the type and quantity of hazardous materials involved.

- a. The **Crime Scene Boundary** defines the crime scene. The crime scene may include the areas which are referred to in technical operations as the "working point" or "red zone." Access to the crime scene may be restricted by federal, state, and local law enforcement. Response activities within the crime scene may require special procedures in order to protect evidence collection.
- b. The **Hazardous Materials Boundary** defines the hazardous materials site, which may be referred to in technical operations as the "hot" or "isolation zones". Depending on the spread of contaminants, the hazmat site may include some portion of the crime scene and the surrounding community. Access to the hazmat site may be restricted to response personnel wearing protective clothing and using decontamination procedures.
- c. The **Disaster Boundary** identifies the community-at-risk which may need to take protective actions such as shelter-in-place, evacuation or quarantine. Access into this area may or may not be restricted on the authority of state and local health officials.

4. Terrorist Acts

The more common "acts of terrorism" employed by contemporary terrorist groups and the definitions are:

- a. Arson - Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only a low level of technical knowledge.
- b. Armed Assault / Assassination
 - (1) Armed Assault - Armed assaults can include a wide variety of direct action activities. World wide examples include throwing hand grenades into crowds, rocket attacks on airliners or buildings and the more familiar gun battle or attack.
 - (2) Assassination - A term applied to the killing of prominent persons and symbolic enemies as well as traitors who defect from a group. One method of creating fear and eliminating rivals is simply by killing them. Assassination targets are carefully selected with a strategic purpose and the actual attack has been planned, coordinated and practiced.
- c. Biological Agent Release - Biological agents consist of organisms or chemicals of biological origin that cause death and disease among personnel, animals and plants. Biological agents include anthrax, cholera, plague, botulism and ricin among others. Unlike other terrorist weapons, with the exception of some toxins, any physical manifestation of an attack is likely to be delayed.
- d. Bombing - The improvised explosive device (IED) is the contemporary terrorist's weapon of choice. IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. Other advantages include their attention getting capacity and the ability to control casualties through time of detonation and placement of the device. It is also easily deniable should the action produce undesirable results.

- e. Bomb Threat / Hoaxes - Any terrorist group that has established credibility can employ a hoax with considerable success. A threat against a person's life causes that person and those associated with that individual to devote time and effort to security measures. (A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. False alarms dull the analytical and operational efficiency of key security personnel, thus degrading readiness.)
- f. Chemical Releases - Of the five categories of chemical agents, (nerve, blister, choking, blood and vomiting), nerve gas is undoubtedly the most notorious and dangerous. The nerve gas Sarin was used by the Aum Shinri Kyo group in the Tokyo subway system. The terrorist use of a chemical agent in an enclosed environment such as a subway station, auditorium, sports arena or shopping mall has the potential for creating massive numbers of casualties that will quickly overwhelm response capabilities.
- g. Civil Disturbance - Creating mass, violent disturbances of the public peace in attempts to show the world that the general public does support their cause(s).
- h. Cyber Terrorism - A less violent but increasingly costly tactic is emerging and may be used by terrorists in the future with increasing frequency. As government, business and society in general become increasingly dependent on computers and information technology through the internet, a whole new vulnerability presents itself. Terrorists can use sophisticated hacker skills to enter computer systems remotely to steal, alter or change information contained in databases and operating systems. Cyber terrorists may also attempt to gain control of, or disable, infrastructure components such as dams, utilities or airport radar systems.
- i. Environmental Destruction - Although this tactic has not been widely asserted, the increasing accessibility of sophisticated weapons and explosives to terrorists has the potential to threaten damage to the environment. Examples are: intentional dumping of hazardous chemicals into a city's water supply or the destruction of an oil tanker. Fear of alienation may be a factor that has limited the use of this tactic to date.
- j. Hijacking, Building Seizure, Raids or Attacks on Facilities:
 - (1) Hijacking or Skyjacking - Sometimes employed as a means for escape, hijacking is normally carried out to produce a spectacular hostage situation and to gain media attention to the hijackers' cause. Although trains, buses and ships have been hijacked, aircraft are the preferred target because of their greater mobility and vulnerability.
 - (2) Seizure - A seizure usually involves a building or object that has value in the eyes of the audience. There is some risk to the terrorist because security forces have time to react and may opt to use force to resolve the incident, especially if few or no innocent lives are involved.
 - (3) Raids or Attacks on Facilities - Armed attacks on facilities are usually undertaken for one of three purposes: to gain access to radio or television

broadcast capabilities in order to make a statement; to demonstrate the government's inability to secure critical facilities or national symbols; or for logistical purposes; e.g., robbery of a bank or armory.

- k. **Hostage Taking** - This usually is an overt seizure of one or more individuals with the intent of gaining publicity or other concessions in return for release of the hostage. While dramatic, hostage and hostage barricade situations are risky for the perpetrator when executed in an unfriendly environment. Generally, hostage taking is a well planned operation that involves considerable surveillance, reconnaissance and planning prior to the attack, but it can also be an impromptu situation when some other activity goes bad.
- l. **Kidnapping** - Kidnapping involves the seizure of prominent people. While similar to hostage taking, kidnapping has significant differences. Kidnapping is usually a covert seizure of one or more specific persons until specific demands are met. The perpetrators of the action may not be known for a long time. News media is initially intense but decreases over time. Because of the time involved, successful kidnapping involves elaborate planning and logistics. The risk to the terrorist is less than a hostage situation. Kidnapping for ransom is becoming a favored method for financing terrorist operations in parts of the world.
- m. **Nuclear Release Weapons** - The nuclear terrorist threat consists of improvised nuclear devices (IND) capable of creating a nuclear yield and radiological dispersion devices (RDD). INDs include both nuclear weapons stolen or obtained from a nuclear powers inventory or an improvised device designed and constructed by the terrorists. RDDs involve the inclusion of radioactive material with a conventional explosive device; when the conventional explosive is detonated it contaminates a wide area with the radioactive material.
- n. **Product Tampering / Sabotage** - The objective in most sabotage incidents is to demonstrate how vulnerable society is to terrorist actions. Industrialized societies are more vulnerable to sabotage than less highly developed societies. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and gains immediate public attention. Sabotage of industrial or commercial facilities is one means of identifying the target while making a statement of future intent. Sabotage involves an assortment of methods that can include such diverse techniques ranging from product tampering to spiking trees to discourage their being harvested. The rationale for this tactic can range from extortion to destroying public faith in a product or service.
- o. **Robbery / Attempted Robbery** - Robbery is used as a means to obtain funds to support the terrorist's cause and logistical needs.

B. Assumptions

- 1. Terrorist attacks are usually directed at population centers and buildings or facilities that conduct operations for government, transportation, or industry.

SPECIAL SUBJECTS

2. Terrorist attacks may or may not be preceded by a warning or a threat, and may at first appear to be an ordinary hazardous materials incident.
3. Terrorist attacks may require a vast response effort from all levels of government (federal, state, local).
4. Terrorist attacks may result in large numbers of casualties, including fatalities, physical injuries, and psychological trauma.
5. The attack may be at multiple locations.
6. The attack may be accompanied by fire, explosion, or other acts of sabotage.
7. There may be a booby trap device set off to attract emergency responders, then a second device may be set off for the purpose of injuring the emergency responders.
8. The presence of a chemical or biological agent may not be recognized until some time after casualties occur.
9. There may be a delay in identifying the chemical or biological agent present and in determining the appropriate protective measures.
10. The chemical or biological agent may quickly dissipate or may be long-acting and persistent.
11. Investigation of the cause of the event and those responsible for it are important law enforcement activities.
12. Resources for combating terrorist attacks exist in local, state, and federal governments.
13. Recovery can be complicated by the presence of persistent agents, additional threats, extensive physical damages, and psychological stress.

C. Constraints

1. Local agencies have limited capability for responding to civil disturbances or terrorism events.
2. Hospitals in Jefferson County have limited civilian victim decontamination capability.

IV. POLICY**Jefferson County Emergency Management Council Policy**

- A. Law enforcement will exercise broad lawful authority, within existing capabilities, to protect life and property threatened by civil disturbance or terrorism incidents, to include ordering evacuations, curfews and other necessary actions to contain or control the incident.

- B. Law enforcement agencies will normally retain the role of lead agency and the incident commander until the threat to public safety is abated.
- C. Establish overall direction, control and/or coordination through a Crisis Action Team (CAT) or an Emergency Operations Center (EOC) activation to support the response to a civil disturbance or terrorism incident.
- D. Utilize the Incident Command System (ICS) as the organizational basis for response to a civil disturbance or terrorist incident.
- E. Ensure that appropriate state and federal agencies will be notified.
- F. This section may be utilized singularly or in conjunction with a CAT or full EOC activation.

V. DEPARTMENTS/AGENCIES/ORGANIZATIONS AND THEIR RESPONSIBILITIES

- A. Jurisdiction's Governing Councils should be prepared to:
 - Establish policy and pass emergency legislation as required to suppress any civil disturbance or disorder affecting the city.
 - Declare a state of emergency.
 - Meet with community leaders in an effort to negotiate differences.
 - Formulate official public relation news releases.
 - Request state assistance.
 - Chief Elected Official's (CEO) will have control of their forces and resources in support of the operational mission.
 - CEO will conduct liaison and coordination with state, local, and private organizations.
 - CEO will notify departments and agencies of the situation.
 - CEO will initiate the emergency mobilization of forces.
- B. Jefferson County Emergency Management Agency
 - Lead local agency for consequence management.
 - Provide crisis monitoring for civil disturbance or terrorist incidents.
 - Activate CAT as required.
 - Provide updates and maintenance of this plan.
 - Responsible for management of the EOC.
 - Develop training and exercise program for civil disturbance or terrorist incidents.
 - Provide EMA staff for key positions at other locations.
 - Advises CEO on declaration of emergency and emergency orders.
 - Ensures that the local response is organized according to ICS .
- C. Law Enforcement Agencies
 - Lead local agency for crisis management.
 - Threat investigation and intelligence.
 - Notify the CEO and EMA.

- Warn the public of any potentially dangerous situation.
- Control access to and prevent looting in damaged or evacuated areas.
- Establish incident command or unified command structure.
- Direct and control the effects of all law enforcement forces deployed to the site of the emergency.
- Secure critical facilities as the situation warrants.
- Prevent and investigate incidents of vandalism, arson, sabotage, sniper attacks, bombing and weapons of mass destruction.
- Collect and disseminate information and intelligence.
- Establish holding areas for processing of violators.
- Coordinate with courts and prosecutors for required initial court appearance within 4 hours of arrest.
- Establish and maintain close liaison with state, county and local law enforcement agencies.
- Furnish liaison personnel to other agencies as required.
- Furnish an information officer to supplement and coordinate official news releases from the public information officer.
- Provide law enforcement and security protection for the personnel and equipment of supporting units.
- Provide law enforcement and specialty teams in cases of hijack, hostage or other emergency situations involving public transportation service.
- Coordination and cooperation with state and federal law enforcement agencies.

D. Public Works

- Assist in providing barricades for riot control.
- Remove barricades erected by rioters.
- Provide debris clearance.
- Provide assistance in traffic control and evacuation as necessary.
- Advise on traffic control matters.
- Advise on closing of streets and thoroughfares.
- Determine detour routes.
- Provide other assistance as required.

E. MAX Public Transit

- Assist and cooperate with the law enforcement in detouring bus routes and providing buses.
- Provide radio contact to public transportation vehicles in emergency situations and assist, if requested, in locating vehicles via road supervision and transit security personnel.

F. Public Information Officer

- Obtain information about the civil disturbance/terrorism from all agencies' information officer and other sources.
- Prepare official news releases.
- Establish a Joint Information Center (JIC).

G. Community Development Department

- Establish contact with the EOC and advise on community activity.
- Assist in identifying the short and long range causes and areas of tension, and work to eliminate them.
- Work with community leaders to diffuse tensions in the community.

H. City and County Attorney

- Advise on legal matters pertaining to a civil disturbance.
- Have a representative present in the courts to authorize all charges.
- Prepare emergency declarations and proclamations.

I. Courts

- Expand court operations in order to expedite the processing of the increased number of cases presented for hearing as a result of the event.
- Provide, if possible, a temporary location where court functions will be carried out.
- Provide court clerical personnel to assist in preparing charges as required.

J. Fire Services / Emergency Medical Services

- Establish on-site liaison at the law enforcement command post.
- Receive clearance from command post for fire services forces to enter the affected areas.
- Conduct on-site operations relating to safety and security under the direction of the command post.
- Coordinate fire service response to hazmat incidents.
- Coordinate local search and rescue efforts.
- Operate with fire suppression strategy as directed by the EOC and the command officer at the scene.
- Provide emergency medical services as permitted by safety and security precautions.
- Coordinate dispatch policies with the EOC.
- Assume special assignments as determined by the fire service's representative at the EOC.
- Assign fire investigative teams to coordinate activities with law enforcement relating to arson.

K. Fleet Management

- Procure emergency transportation as required by the situation from either public or private sources.

L. Water Works

- Provide security at all water treatment plants, pumping stations, and reservoirs with assistance of law enforcement and outside contractors as necessary.
- Fill all reservoirs to capacity.
- Shut down water service where necessary.
- Provide domestic water by whatever means possible, in areas where normal service has been disrupted.

M. Human Services Agencies

- Establish contact with the EOC and advise on community activity.
- Keep lines of communication open with community leaders.
- Schedule meetings with community leaders to negotiate differences.

N. Jefferson County Department of Health

1. Medical / Health

- Monitor and investigate public health threats.
- Initiate public health alerts and emergencies.
- Maintain and operate radiological detection equipment.
- Modify existing protocols to address terrorist response issues.
- Assist in development of medical first responder guidelines.
- Responsible for refresher training procedures.
- Coordinate with other disciplines, such as hazardous materials, law enforcement and fire services.
- Identify technical support team requirements.
- Establish mutual aid procedures.
- Determine logistical support requirements.
- Research first responder security and personal protection criteria.
- Set procedures to access privately owned and operated medical assets.
- Assist with the development of decontamination procedures.
- Responsible for mass casualty incident (MCI) concerns.

2. Mental Health

- Staff training in disasters, terrorism, and emergency management.
- Public information about mental health.
- Mental health support services.
- Mental health follow-up programs.
- Integration of mental health with other programs.
- Support to care and shelter and other operations.
- Stress management programs for responders.

VI. CONCEPT OF OPERATIONS

A terrorist threat or actual incident will likely require the response by the State and Federal governments. However, Jefferson County and its local governments will still play a key role in Crisis Management and the full role, initially, in Consequence Management, with that role continuing throughout. When the response involves multiple levels of government, the coordination between and among such agencies is an absolute necessity. The Incident Command System (ICS) is a means for ensuring that the required close coordination is realized. Jefferson County and State government will organize its response to a terrorist threat/incident according to the Incident Command System.

Crisis Management, the purview of law enforcement, may operate from a general threat, to a credible threat, through the incident. Consequence Management, the purview of

all response agencies, may operate before, during, and after an incident, and continue until demobilization of emergency operations.

A. Notification

The following outlines potential notification procedures. This sequence may need to be modified any time there is a change in status, such as verification of a credible threat, information updates, and notification of an actual event. Additional agencies or organizations should be added as appropriate.

1. Notification Actions - City Level

Notify:

- Local FBI Office.
- Jefferson County EMA.
- City departments: police, fire, EMS, threat assessment unit as appropriate. Include other city staff as necessary.
- Other levels (county, state and federal) dependent upon nature of threat and security considerations.

2. Notification Actions - County Level

Notify:

- Local FBI Office.
- Jefferson County EMA.
- City or cities that may be impacted.
- County departments: sheriff, fire, medical, and threat assessment unit as appropriate. Include other county staff as necessary.
- Appropriate state agencies.
- Other levels (state and federal) dependent upon nature of threat and security considerations.

3. Notification Actions - State Level

Notify:

- Local FBI Office.
- Local Law Enforcement Agencies.
- Jefferson County EMA.
- Appropriate State Agencies.
- Other levels (Local, Federal) dependent upon nature of threat and security considerations.

4. Notification Actions - Federal Level

Notify:

- State Law Enforcement Agency.
- AEMA.

- Appropriate Federal Agencies.
- Other levels (Local and State) dependent upon nature of threat and security considerations.

B. Response

1. Protecting Emergency Responders

Emergency personnel first responding to a terrorist incident must be protected from the various hazards that a terrorist incident can produce. These include:

Mechanical Hazard - Any type of mechanical harm causing trauma (includes gunshot wounds, bomb fragments or shrapnel).

Etiological Hazard - Disease causing material including: bacteria (e.g., anthrax), rickettsias (e.g., Q fever), viruses (e.g., hemorrhagic fever), and toxins (e.g., ricin or botulinus).

Thermal Hazard - From both extreme heat and cold (e.g., burning liquids or metals like magnesium; cryogenic materials such as liquid oxygen).

Chemical Hazard - Toxic or corrosive substances (e.g., acids such as sulfuric or hydrochloric; caustics such as ammonium hydroxide; toxic substances such as nerve agents, pesticides, or other chemical agents).

Radiological Hazard - Alpha, beta, and gamma radiation from nuclear material.

Asphyxiation Hazard - Lack of oxygen in the atmosphere due to displacement by heavier-than-air vapors or depletion by a chemical reaction such as burning.

Though the type of protection required varies from hazard to hazard, there are three basic principles of protection that apply to all hazards: time, distance, and shielding.

- Time.** Spend the shortest amount of time possible in the hazard area or exposed to the hazard. Use techniques such as rapid entries to execute reconnaissance or rescue. Rotate personnel in the hazard area. The less time spent in the affected area, the less likely you would be injured. Minimizing time spent in the affected area will also reduce the chance of contaminating the crime scene.
- Distance.** Maximize the distance from the hazard area or the projected hazard area. For chemical hazards recommended distances are included in the North American Emergency Response Guidebook (NAERG).
- Shielding.** Use appropriate shielding to address specific hazards. Shielding can include vehicles, buildings, chemical protective clothing, and personnel protective equipment.

NOTE: Detailed information on protection from specified terrorist incidents and hazards is contained in Appendix 1 of this Section.

2. Scene Control

a. Initial Considerations

Approaching a criminal event that has been created by an act of terrorism presents unique challenges to the responder. To effectively implement scene control and ensure public safety, emergency responders must quickly and accurately evaluate the incident area and determine the severity of danger. Once the magnitude of the incident is realized, attempts to **isolate the danger** can begin. Establishing control (work) zones early will enhance public protection efforts.

- (1) Initially, when response resources are limited, isolating the hazard area and controlling a mass exodus of panicked and contaminated people will likely overwhelm the best efforts of the first arriving responders.
- (2) Terrorists may still be lurking nearby waiting for responders to arrive, or could be among the injured. If this is suspected, initial scene control will likely be delayed and dictated by law enforcement activities.
- (3) Anticipate the potential for multiple hazard locations. Responders may have to define outer and inner operational perimeters. There may exist several hazards within the outer perimeter that must be isolated, especially when victims are scattered throughout the boundaries of the incident, or multiple targets contain dangers.
- (4) Controlling the scene, isolating hazards and attempting to conduct controlled evacuations will be resource intensive. Inordinate security may be needed for the event, so responders should request additional assistance early.
- (5) After a bombing, access to the scene may be limited due to rubble or debris. Police activity may make it difficult to establish access and exit avenues for operations.

b. Perimeter Control

- (1) Recognizing and evaluating dangers is critical to implementing perimeter control. Adequately evaluating potential harm will guide decisions and considerations for “stand off” distances, or establishing “work zones.”
 - Take time to perform an adequate size-up.
 - Better to overestimate the perimeter than underestimate, it is easier to reduce the perimeter instead of increasing it after operations are set up.
- (2) Depending on the size and complexity of the incident, the boundaries may need to be divided or identified as having “outer” and “inner” perimeters.

- The outer perimeter is the most distant control point or boundary of the incident. It is used to restrict all public access to the incident.
 - The inner perimeter isolates known hazards within the outer perimeter. It is used to control the movement of responders.
 - Types of terrorist incidents that may require outer and inner perimeter control include:
 - Improvised explosive devices;
 - Chemical or biological dispersion devices;
 - Radioactive contamination.
- (3) Perimeter control may be influenced by the following components:
- Amount and type of resources on-hand;
 - Capability of available resources (training level);
 - Ability of the resources to provide self-protection (personnel protective equipment);
 - Size and configuration of the incident; and
 - Stability of the incident.
- (4) Establish the standard “control zones” within the outer perimeter. These zones include the:
- Hot (exclusion) zone (exceptional access);
 - Warm zone (contamination reduction corridor); and
 - Cold (support) zone (staging area).
- (5) Because of the potential for secondary and tertiary events, the perimeter and control zones should be mapped. Therefore, if the incidents escalate, boundaries can be expanded using established reference points that are familiar to on-scene responders. Mapping components should include:
- Topography;
 - Structures/landmarks;
 - Access and egress points; and
 - Perimeter boundaries.
- (6) Using detection and monitoring equipment to identify perimeter and work zone boundaries has limitations:

- Responders must attempt to identify “clean” areas as well as hazardous areas. This is usually accomplished by using detection and monitoring equipment. However, equipment designed to detect hazardous materials may not be immediately available to first responders.
- Unlike chemical and/or biological detectors, radiological detection equipment and trained operators are available from the Jefferson County Emergency Management Agency.

(7) Isolation/Standoff Distance Considerations

- First, identify the problem from initial incident information (dispatcher reports) and outward warning signs and detection clues.
- Determine isolation area based upon these factors:
 - Potential of harm to life, critical systems, and property;
 - Topography;
 - Meteorological factors;
 - Resources available to implement tactical operations.
- Access reference materials such as the NAERG to determine initial isolation and protection distances.
- When limited information is available pertaining to the agent, Guide 111 in the NAERG recommends minimal isolation distances of 50 to 100 meters (160 to 330 ft.) in all directions.
- If responders suspect radioactive materials, use appropriate detection equipment with trained operators in determining isolation distances. Monitoring for radioactive materials at any bombing event should be done routinely. Monitoring is the only way to detect the presence of radiation at the scene.

3. Public Protection Consideration

a. Overview

Public safety will largely depend on the ability of responders to effectively conduct a hazard and risk analysis of the affected population. The same basic strategies used by responders to protect the public during a hazardous materials incident can be applied to a terrorist event. First arriving responders may be required to make rapid decisions that apply to implementing public protection measures because of escalating dangers. This being the case, those responders will need to base decisions on information gathered during the primary **size-up**. This can be a challenging task at any significant incident when so many demands are placed upon first arriving units. Remember, **size-up** is a continuous process of gathering and using information to make the best decision at a particular point in time.

For a major terrorist incident, the following options should be considered in defining the approach to protecting the public:

- (1) Evacuation.
- (2) Shelter-in-place.
- (3) A combination of evacuation and shelter-in-place.

b. Evacuation

Evacuating the public from a hazard is a decision based on information that indicates the public is at greater risk by remaining in or near the hazard area. The types of information that should be considered in the decision to evacuate should include the following:

- (1) The degree or severity of public dangers or threats as a result of the hazard.
- (2) The number of individuals or population area affected by the hazard.
- (3) Availability of the resources needed to evacuate the affected population including:
 - Additional fire/EMS/police personnel .
 - Transportation vehicles including school buses, privately-owned vehicles or public mass transit.
- (4) Means available to notify the public and provide emergency instructions before and during the evacuation, including:
 - Local broadcast media (Emergency Alert System).
 - NOAA Weather Radio.
 - Route alerting via mobile address systems.
 - Sirens.
 - Door to door alerting.
- (5) Safe passage for the evacuees, including:
 - Adequate time and opportunity to conduct the evacuation.
 - Evacuation route monitoring.
 - Ability to reroute traffic due to congestion.
 - Availability of shelters.

(6) Special needs of the evacuees:

- The need to assist special facilities (e.g., hospitals, nursing homes, prisons) in evacuating.
- The need to alert and warn the hearing impaired and provide evacuation assistance to the mobility impaired.

(7) The ability to provide shelter and sustenance to evacuees including:

- Adequately staffed shelters with feeding and lavatory facilities.
- The provision of medical care to evacuees in need.

c. Shelter-in-place

Shelter-in-place is the advising of the affected population to remain indoors and seek protection within the structure that they occupy or in a nearby structure. The decision to shelter-in-place is based upon the analysis of the hazard. If the danger to the public is determined to be less by shelter-in-place, rather than by evacuating, then shelter-in-place should be carried out. With certain hazards (i.e., short term airborne chemical or radiation hazards or line-of-sight exposure to explosives) the best decision may be to shelter-in-place. Distinct advantages of shelter-in-place over evacuation are the relative short time and ease of implementation. Remember, as long as there remains a danger, hazards and risks must be continuously evaluated. When considering shelter-in-place include the following:

- (1) The risks of shelter-in-place vs. evacuation.
- (2) The availability of resources.
- (3) The time available to take protective action.
- (4) The level of public understanding of the shelter-in-place concept.

For explosion, shelter-in-place can be enhanced by seeking the most protective refuge in the structure. For chemical, radiation, and some biological hazards, shelter-in-place may be enhanced by reducing the indoor-outdoor air exchange rate.

d. Combination of Both Protective Actions

There may be circumstances when using both evacuation and shelter-in-place would be appropriate. For example, when time or resources cannot support the immediate need to evacuate a large population, only those closest to the hazard, and at the greatest danger, could be instructed to evacuate, while people not in the immediate area would be advised to shelter-in-place.

4. Scene Security Considerations

- a. The agency assigned site security responsibilities will likely vary according to the location and scope of the incident and the resources available.
- b. Whenever there is an ongoing or unstable criminal activity present, law enforcement officials should dictate security measures for scene control.
- c. As the incident becomes more defined and more stable (intermediate phase), the shift from a combination of police and other (non-police) personnel in control of the perimeter should begin to transition to all law enforcement.
- d. If the incident is of such magnitude that response activities may continue for days, the use of National Guard units should be considered for perimeter security and control. National Guard support can only be obtained if requested through Alabama Emergency Management Agency by Jefferson County Emergency Management Agency.

5. Tactical Considerations

When an emergency responder approaches any type of suspicious incident, the responder should do so in a cautious manner with all senses alert for warning signs and detection clues. The following rules should always apply.

- a. Always approach the scene utilizing protective clothing and equipment.
- b. Be alert for outward warning signs that may indicate the type of danger present, such as:
 - (1) Casualties resulting from no apparent reason.
 - (2) Signs and symptoms indicating chemical exposure.
 - (3) Obvious signs of criminal activity, such as weapons on the scene.
 - (4) Suspicious vehicles or packages.
 - (5) Pre-incident verbal or written warnings.
- c. Properly stage vehicles. During emergency conditions (especially if the incident has created large scale public chaos and panic) responders must realize when approaching the event, conditions may not provide the most ideal locations to stage vehicles and apparatus. When possible, consider the following:
 - (1) If practical, position first-in vehicles and responders upwind and uphill.
 - (2) Direct supporting responders to approach from upwind and uphill.
 - (3) Avoid 'stacking' vehicles where they interfere with each other's evacuation route.
 - (4) Avoid line-of-sight staging with suspected explosive devices.

- (5) Strictly enforce staging instructions.
 - (6) Consider having vehicles back into position so that they may leave the scene quickly.
- d. Avoid vapor clouds, mist and unknown liquid.
 - e. Initially, assign at least one responder to observe ongoing activities surrounding your operating position. This person should be alert for criminal activities and the potential for secondary events.
 - f. Plan tentative escape routes for emergency personnel and refuge assembly points.
 - g. Prepare for emergency decontamination on arrival and during all phases of the incident.

Each response agency should have plans for emergency decon of large (mass decon) and small groups of contaminated persons. These plans should be developed and maintained with the assistance of the Jefferson County Department of Health in order to provide technically correct decon procedures without incurring potential liability for privacy violations.

NOTE: Detailed information on tactical considerations from specified terrorist incidents and hazards is contained in Appendix 2 of this Section.

6. Incident Command for Terrorist Incidents

a. Overview

Terrorism is more challenging to manage than most other emergency events. It presents or requires the following:

(1) Coordination of multiple response agencies.

- The incident commander (IC) must ensure that all participating agencies (local, state, and federal) are effectively communicating within the designated command structure.
- Regular planning sessions should be conducted to review the progress of assigned tasks and to incorporate new resources as they engage or disengage from the incident.
- When multiple agencies are operating on site, the IC must request or appoint a representative or liaison for each.

(2) Unique scene control/security issues.

- Ongoing criminal activities will likely impact scene control initiatives. Police may limit or restrict access to the scene due to security concerns.

- Due to the dynamic nature of criminal activity, anticipate that the incident perimeter will be larger than would be expected simply due to the incident scope.

(3) Special awareness that responders may be an intended target.

- Consider that terrorists may still be on the scene, waiting for responders to arrive. The intent could be to add responders to the victim list.

(4) Specialized resources.

- Terrorist events will generate responses from many agencies. Some of the response teams will provide personnel who are specially trained and equipped to support operational objectives. Examples include the FBI Hazardous Materials Response Unit and Law Enforcement Bomb Disposal Teams.

(5) Crime scene considerations (evidential preservation).

- Responders working in the confines of a crime scene must respect the mission of law enforcement investigators. Assist the mission by identifying and preserving potential evidence whenever encountered or suspected.

b. The Role of the Incident Commander

The IC must safely, effectively and efficiently manage response resources to achieve the most favorable incident outcomes possible.

(1) Follow the SEE principle.

Safe -No one gets hurt.

Effective -Everyone works toward stated objectives.

Efficient -All resources are utilized to maximum benefit.

(2) Management of the incident is based on two components:

- Establishing and updating priorities.
 - Life safety
 - Incident stabilization
 - Property and environmental conservation
 - Investigation of cause and origin
- Continual size-up based on all available information.
 - Present situation
 - Predicted behavior

(3) Incident Command responsibilities may include, but are not limited to:

- Establishing command.
 - Hazard and risk assessment.
 - Notifications.
 - Developing and implementing site safety.
 - Ensuring responder protection levels.
 - Public protection.
 - Developing and implementing integrated Incident Action Plans (IAP).
 - Controlling hazards.
 - Requesting specialized resources.
 - Resource management.
 - Evaluating progress.
 - Logistical support.
 - Information control.
 - Incident termination.
- (4) Command and control issues at terrorist incidents will likely involve a unified command system in order to properly coordinate the various agencies and authorities involved in responding to the incident. Some key agencies may include:
- Local Government.
 - Local Fire Department
 - Local Law Enforcement Agencies
 - Jefferson County Sheriff Department
 - Jefferson County Department of Health
 - Jefferson County Emergency Management Agency
- This plan designates the local law enforcement agency as the lead local agency for crisis management for terrorist incidents affecting Jefferson County. It also designates the Jefferson County Emergency Management Agency as the lead agency for consequence management.
- State
 - Department of Public Safety
 - Department of Health
 - Department of Environmental Management

- State Fire Marshal's Office
- Emergency Management Agency

The Alabama Domestic Preparedness Plan identifies the Department of Public Safety as the lead state agency for crisis management for terrorists incidents. The designation of the lead state agency for consequence management is contingent upon the actual event and will be designated by the Alabama Emergency Management Agency at the time of the incident. AEMA is designated as the lead state agency for coordination of state-level emergency response.

- Federal
 - Federal Bureau of Investigation (FBI)
 - Federal Emergency Management Agency (FEMA)

Presidential Decision Directive-39 identifies the FBI as the lead agency for federal crisis management during terrorist incidents involving nuclear, biological, or chemical materials. It identifies FEMA as the lead agency for federal consequence management during terrorist incidents involving nuclear, biological, or chemical materials.

(5) Transition of Incident Command

The Incident Commander for a major terrorist incident will likely be a local law official, initially. As state and federal assistance arrives and the scope of the response grows more complex, the need to transition from incident command to unified command may become obvious. This transition must be accepted by all and Jefferson County officials will support such a transition.

(6) Termination of the Incident

Termination procedures include debriefing all response participants. For terrorist incidents, debriefing sessions are especially important to responders that are unfamiliar with weapons of mass destruction. Recognize the potential for psychological impacts for several reasons:

- Most responders are not accustomed to dealing with chemical and biological warfare agents;
- Responders may have been the intended target;
- Exposure concerns may cause post-incident stress

(7) Recovery

Presumably, response/recovery incurred expenses will be borne by the impacted jurisdiction without a federal disaster declaration.

The President may declare a "federal emergency" under Title V of the Stafford Act. The emergency declaration only covers disaster-related emergency debris removal and emergency protective measures. As disaster damage information is collected and evaluated, the President may change the "federal emergency" to a "major disaster" declaration. The recovery efforts of the federal government are guided by the Stafford Act.

If a terrorist incident creates a nuclear emergency which results in contamination, site restoration will be based on technical considerations (primarily health and safety) at the time of the event. The Price-Anderson Act, which is designed primarily to address cost recovery for accidents at commercial nuclear plants, including transport of nuclear fuels, does not specifically address terrorist theft, sabotage, or diversion of nuclear materials.

VII. TRAINING / EXERCISES

A. Training

Law Enforcement agencies and the Jefferson County EMA, along with other local organizations will conduct internal training on Civil disturbance/terrorism events. See Attachment B for generic master training and exercise schedule.

B. Exercises

Drills and exercises are conducted to maintain proficiency. Civil disturbance/terrorism situations are worked into normal disaster preparedness exercises, if appropriate for the responder needs and if within capabilities of available personnel at the time of the exercise. Lack of funding and personnel time constraints do not permit the vigorous exercise schedule envisioned by the Federal Government.

VIII. ADMINISTRATION AND LOGISTICS

A. The City and County Finance Departments will:

1. Prepare to resupply expendable items unique to civil disturbance/terrorism control.
2. Prepare to obtain additional protective equipment.
3. Prepare to establish an emergency resupply of medical expendables.

B. Communications.

1. The support forces will furnish their own communications system.
2. Maintain radio contact with the incident command post or the EOC.

C. Call-Up or Notification Lists.

1. Lists will be maintained by each department and will be updated as required.

IX. APPENDICES AND/OR REFERENCES.

A. Attachments

1. Attachment A: Terrorism Incident Management Functions
2. Attachment B: Master Training and Exercise Schedule
3. Attachment C: Potential Terrorism Response
4. Attachment D: Terrorism Response Actions

B. Appendices:

1. Appendix 1: Specific Terrorism Hazards and Personnel Protection
2. Appendix 2: Response Tactics for Specific Terrorism Hazards
3. Appendix 3: Analysis and Response to Threats of Terrorism
4. Appendix 4: DOD Threat Conditions (Threatcons)
5. Appendix 5: FBI Threat Levels
6. Appendix 6: Threat Data Elements
7. Appendix 7: Unified Command and Incident Management

C. References:

1. California's Local Planning Guidance on Terrorism Response
2. New York State Domestic Preparedness Guidance
3. Emergency Response to Terrorism (FEMA)

**Attachment A
Terrorism Incident Management Functions**

Activities	Management / Command	Operations	Planning / Intelligence	Logistics	Administration
Incident Commander	LE				
Establish Perimeter		FD LE			
Control Access		FD LE PW			
Traffic/Crowd Control		LE PW			
EOC Operations	ADMIN FD EMA LE	LE FD PW P&R	PEP ADMIN	ADMIN PW LE	FIN ADMIN
Evacuation		FD LE		PEP PW	
Notifications		LE FD			
Safeguard Evidence		LE FD			
Public Information	LE FD EMA				
Med/Rescue Operations		FD P&R			
Damage Assessment					
Situation Status		LE FD PW			
Documentation			PEP LE FD PW		
Facilities Management		LE FD PW P&R	ADMIN EMA		FIN

Key: ADMIN - Administration, EMA - Emergency Management Agency, FIN - Finance, FD - Fire Department, LE -Law Enforcement, PEP - Planning, Engineering & Permits, P&R - Parks and Recreation, PW - Public Works

**Attachment B
Master Training and Exercise Schedule**

1st Quarter	2nd Quarter	3rd Quarter	4th Quarter
Awareness Training	First Responders Training	Exercise Preparation	Joint Exercise with County
<p>Two Componets:</p> <ol style="list-style-type: none"> 1. An Orientation to Terrorism 2. Personal Awarness and Protection 	<p>Three Components:</p> <ol style="list-style-type: none"> 1. Refresher on Terriorism Issues 2. Personal Awareness and Protection 3. Discipline Specific Technical Information 	<p>EOC Exercise</p> <p>Scenario to be determined</p> <p>Field Component: NONE</p>	<p>Activation of County EOC</p> <p>Scenario to be determined</p> <p>Field Componet to be determined, depending upon scenario</p>
Audience:	Audience:	Participants:	Participants:
All Staff	FD, PD, PW, Selected Medical Personnel	Staff assigned EOC duties	<p>Staff assigned EOC duties</p> <p>Staff for field Components: To be determined</p>

KEY: FD - Fire Department, PD - Police Department, PW- Public Works

Notes: This is a generic master training schedule. At the beginning of the training year, training coordinators will meet to identify the training emphasis and objectives.

Attachment C Potential Terrorism Response

Purpose: To outline various terrorism response organizations.

This table describes the potential terrorism response organizations at different levels of government. It is broken into two periods: 1) Preparedness, and 2) Notification of Potential / Actual Events.

Government Level	Preparedness	Notification of Potential / Actual Events
Federal	FEMA National, FEMA Region IV, FBI Field Offices	FEMA National, FEMA Region IV, Regional Operations Center (ROC) Disaster Recovery Office (DRC) FBI Strategic Information Operations Center (SIOC) (Washington, DC) FBI Joint Operations Center (JOC) (Operated by FBI Field Office(s)) ¹
State	State Committee on Terrorism (SCOT) AEMA State Agencies	State Committee on Terrorism (SCOT) AEMA Emergency Operations Center (SEOC) State Agencies Departmental Operations Center (DOCs)
Local Government	Local Government (may include provisions for terrorist threat assessment group or terrorism working group (TWG))	Local Government EOC(s) (may include activation of terrorist threat assessment group or elements of the terrorism working group (TWG))
Field		Unified Command FBI Command Post Metropolitan Medical Strike Team (MMSTs) First Responders (Law, Fire & Rescue, Medical, Public Works) Various special purpose teams, such as the National Guard Rapid Assessment and Initial Detection (RAID) Teams

¹ Exact Location to be Determined

**Attachment D
Terrorist Response Actions**

Crisis Management	Consequence Management
Threat notification and assessment within Law Enforcement community	Activation of EOC and SEOC as applicable
Activation of threat assessment organizations, such as the State Committee on Terrorism (SCOT) or the Terrorism Early Warning (TEW)	First Responders deployed to Incident Site(s)
Activation of selected elements of the emergency response organization based upon the situation. May include partial activation of EOC or SEOC.	Unified Command activated at Incident Site(s).
Alerting of key First Responders at the local level, if warranted by situation.	FBI JOC may collocate with impacted jurisdiction's EOC's. Continued threat analysis.
Time-critical refresher training, if applicable.	Evidence collection at site(s).
Initiation of Consequence Management Planning as applicable.	Mutual Aid System activated as necessary (Law, Coroner, Fire and Rescue, Hazardous Materials, Medical / Health, Mental Health, Public Works, Utilities).
Review of evidence gathering procedures and protocols, if applicable	Public information protocols and procedures activated.
FBI activates JOC.	FEMA becomes involved in Consequence Management.

Notes: Crisis Management and Consequence Management time frames may overlap. Crisis and Consequence Management activities will require close coordination.

Appendix 1

Specific Terrorism Hazards and Personnel Protective Measures

I. FIREARMS

A. Overview

Armed attack incidents can include many different scenarios and types of weapons. Harm occurs from physical trauma inflicted from the weapon(s). Terrorists generally utilize weapons that can kill the largest number of persons in the shortest amount of time.

B. Types of Harm

1. Primary: Mechanical

Historically the weapons of choice have been 9 mm semi-automatic pistols, 9 mm machine guns and AK-47 type assault rifles.

2. Secondary: Etiological (disease causing)

Etiological harm may come from contact with blood and other bodily fluids.

C. Implementing Personnel Protective Measures

1. **Time** - Until the scene has been secured by law enforcement officials any time spent in the area should be kept to an *extreme* minimum. Time spent in the unsecured area should only be done by trained responders executing clear tactical objectives.
2. **Distance** - Until the scene has been secured by law enforcement officials, responders should keep an approximate distance of ½ to 1 mile from the shooter's location. Determining the exact distance will be based on topography and the individual situation. The point is to utilize distance as much as possible. Be aware that projectiles from high-powered rifles can travel distances greater than one mile.
3. **Shielding** - Implementing shielding from an armed attack can be accomplished by utilizing physical objects such as buildings and response vehicles. In some high risk areas and situations departments have issued protective vests and helmets. Shielding at an armed attack needs to include both horizontal shielding and vertical cover. Projectiles falling from above, as well as shots fired from elevated structures can bypass horizontal shielding. Responders should utilize comprehensive shielding as projectiles can ricochet from any direction.

II. EXPLOSION

A. Overview

1. Size and Target

Bombing incidents can involve multiple devices from small pipe bombs to large vehicle bombs. The incident may involve an attack against a fixed target or a group of people such as emergency responders. The incident may be an isolated event or may involve secondary devices, booby traps or suicide bombers.

2. Materials Used

Materials involved will always include some form of explosives. However, the detonation may be designed to disperse biological, chemical or radiological materials. The type of bomb involved may be an improvised explosive device or a commercially manufactured explosive.

3. Detonation Methods

The bomb may be activated by a timing device or equipped with various switches that can be activated by light, heat, pressure, movement or radio transmission.

4. Special Considerations

Currently, bombs are the weapons most frequently used by terrorists. It is important to note that one of the bomb victims may be the bomber. For this reason, victims may be searched for weapons prior to transport.

B. Types of Harm

1. Thermal

This would apply to individuals exposed to the heat generated by the detonation. It is usually not an ongoing risk unless there are unexploded materials present.

2. Radiological

If the device was designed for the purpose of dispersing radiological contamination or detonated in an area containing radiological materials, this will present a continuing hazard.

3. Chemical

Chemical hazards can come from products created as a result of the explosive reaction, from chemicals already present at the detonation site, or which have been included in the device for the purpose of being dispersed. All of these potential hazards must be addressed by responders.

4. Etiological

This will be a primary risk if the device is used as a dispersion mechanism. Otherwise, it is always a secondary risk due to mechanical trauma.

5. Mechanical

Mechanical harm can result from blast over pressure, shockwaves and fragmentation.

C. Implementing protective measures

1. Time

a. Pre-blast

Attempting to use time as a protective measure in a pre-blast situation is a gamble. Once detonation starts, harm will occur almost instantaneously.

b. Post-blast

Minimizing exposure time in the affected area will assist in keeping exposure to hazards as low as possible. Work time in the affected area should be kept at a minimum until the area has been evaluated by specialized teams. These teams will search the area for mechanical hazards, unexploded material, radiological hazards, chemical hazards, biological hazards, secondary devices and booby traps.

2. Distance

a. Pre-blast

Determining the appropriate distance from a suspected explosive device is difficult. Responders must consider the size and estimated power of the device, topography of the scene and estimation of harm in the event of detonation. Guide 112 in the NAERG (which provides guidance for Class A and B explosives) states "May explode and throw fragments 1600 meters (1 mile) or more if fire reaches cargo." For public safety at non-fire situations it recommends isolating the area for at least 500 meters (1/3 mile) in all directions. The NAERG further recommends not operating radio transmitters within 100 meters (330 feet) of the device.

b. Post-blast

These incidents may involve a large area. Maintaining a proper distance from the effected area until it has been evaluated by specialized teams is important.

3. Shielding

a. Pre-blast

Implementing shielding at the scene of a bombing incident can be accomplished by utilizing physical objects such as buildings and response vehicles. If practical, keep out of the line of sight of the scene and stay away from windows.

b. Post-blast

May require the use of respiratory protection and protective clothing.

III. BIOLOGICAL AGENTS

A. Overview:

Biological incidents will present themselves as either a focused emergency response or a public health emergency. Materials include bacteria, rickettsia, viruses or toxins. These materials are inhaled or ingested into the body to cause harm.

B. Types of harm

1. Primary: Etiological

These materials are classified as Class 6 Hazardous Materials by the US Department of Transportation.

2. Secondary: Chemical

Possible secondary hazard (e.g., at the scene of a clandestine laboratory).

3. Secondary: Mechanical

Possible secondary hazard where explosives have been used to disperse the agent.

C. Implementing self-protective measures

1. **Time** - Keep exposure time and product contact to a minimum.

2. **Distance** - Keep an appropriate distance from the actual biological material. Stay up wind, uphill and away from contaminated areas and casualties if you don't have the appropriate protection.

3. **Shielding** - Implementing appropriate shielding in the form of respiratory protection and protective clothing.

IV. CHEMICAL AGENTS

A. Overview:

Chemical incidents can include many hazardous materials classes. Materials can be inhaled, ingested, absorbed, or injected. Materials can include industrial, chemical, or warfare type agents.

B. Types of Harm

1. Primary: Chemical

Chemical hazards, of course, include a wide variety of effects including corrosive, reactivity, and a variety of systemic effects which may attack the central nervous system, cardiovascular system, respiratory system and other bodily functions.

2. Secondary: Thermal

Many chemical reactions create heat. Also, the chemicals involved may be flammable.

3. Secondary: Asphyxiation

Some chemical reactions may deplete oxygen or create gases that displace oxygen.

4. Secondary: Mechanical

Corrosive chemicals like strong acids can weaken structural elements.

C. Implementing protective measures

1. **Time** - Keep exposure time and product contact time to a minimum.
2. **Distance** - Keep an appropriate distance from the actual chemical. Stay up-wind, uphill and away from contaminated areas and casualties if one doesn't have the appropriate protection.
3. **Shielding** - Implement appropriate shielding in the form of respiratory protection and protective clothing.

V. INCENDIARY DEVICES

A. Overview

Incendiary incidents involve flammable devices that are either stationary or hand-thrown. Incendiary devices are used in approximately 20-25% of all bombing incidents in the United States and can include many different chemicals and flammable or explosive devices.

B. Types of harm

1. Primary: Thermal
2. Secondary: Asphyxiation

Asphyxiation is always a possibility due to the fact that burning depletes oxygen.

3. Secondary: Chemical

The incendiary material may release a chemical hazard or other fuels present may generate chemical hazards.

4. Secondary: Mechanical

Secondary from structural damage, thrown devices or secondary events or explosions.

C. Implementing Self-Protective Measures:

1. **Time** - Keep exposure time in the affected area and product contact time to a minimum.
2. **Distance** - Keep an appropriate distance from any chemicals. Stay up wind, up-hill and away from contaminated areas and casualties if one doesn't have the appropriate protection.
3. **Shielding** - Implement appropriate shielding in the form of respiratory protection and protective clothing.

VI. NUCLEAR DEVICES

A. Overview

Terrorist nuclear incidents are most likely going to involve the use of an explosive dispersion device or any other means to spread nuclear materials. Intelligence sources report that the use of a nuclear fission device to cause a nuclear detonation is highly unlikely if not nearly impossible. Identifying a nuclear incident may be difficult due to the fact that radiation cannot be detected by the senses and that symptoms of radiological exposure are generally delayed for hours or days.

B. Types of Harm

1. Primary: Radiological

Due to the nature of radiological materials, this will present an ongoing hazard, the scope of which will only be determined when the amount and identity of the substance involved is ascertained.

2. Secondary: Chemical

Many radiological substances are also chemical hazards. This is an area that may be overlooked by responders concentrating on radiation effects.

C. Implementing Protective Measures

Remember that radiological detection equipment is the best method to determine if your self-protective measures are effective and appropriate.

1. **Time** - Spend the shortest amount of time in the suspected contaminated area.
2. **Distance** - Keep an appropriate distance from the suspected contaminated area. The NAERG, page 161, section on radiological materials recommends to isolate the area for at least 25 to 50 meters (80 to 160 feet) in all directions and to stay upwind.
3. **Shielding** - Implementing shielding at the scene of a radiological incident can be accomplished by utilizing physical objects such as buildings and response vehicles. The penetration effects of radiation are dependent upon the type of material and the nature of the radiation emitted. As a rule of thumb, keep as much mass between the responder(s) and suspected radiological materials as possible.
4. Avoiding Internal Contamination

Do not eat or drink in any area with a suspected or confirmed radiological hazard.

Appendix 2

Response Tactics For Specific Terrorism Hazards

This appendix addresses tactical issues for Biological, Nuclear, Incendiary, Chemical, and Explosives incidents.

I. BIOLOGICAL AGENTS

A. Introduction

Biological agents can be either disease-causing organisms (bacteria, rickettsia or viruses) or toxins produced by living organisms. Biological agents are generally split into three groups:

1. Bacteria and Rickettsia - Single celled organisms which cause a variety of diseases in animals, plants and humans. They may also produce extremely potent toxins inside the human body. Rickettsia live inside individual cells.
2. Viruses - Much smaller than bacteria, and use the reproductive mechanism of host cells to create more viruses.
3. Toxins - Potent poisons produced by a variety of living organisms including bacteria, plants, and animals. Biological toxins are some of the most toxic substances known. Ricin is 10,000 times more toxic than the sarin nerve agent used in the Tokyo subway attack.

B. How are Biological Agents Disseminated?

There are a wide variety of means to disseminate biological agents.

1. Aerosol dispersion to produce airborne hazard.

An agricultural sprayer can be used to spray just about anything. A typical commercial unit has dozens of nozzles which produce a particle size between 2 and 6 microns.

This is an ideal size for spreading biological agents such as anthrax spores. There are no restrictions on sale or purchase of this type of unit and it is sold all over the world for agricultural use.

2. Oral dissemination via contamination of food, water, or medicine.

Terrorists sprayed salmonella on salad bars in the Northwest which caused over 700 people to become ill. These same terrorists could have used ricin or some other deadly agent that could have killed those whom the salmonella merely made ill.

3. Dermal exposure by direct contact or injection.

Georgi Markov was a Bulgarian journalist who wrote in 1968 about corruption in high government offices in Bulgaria. He was forced to flee Bulgaria for Italy and eventually England. While living in London he continued his reports on Bulgaria and its problems as a reporter for Radio Free Europe. One morning while waiting for a bus, he was jabbed in the thigh with an umbrella. His health quickly deteriorated and he died four days later. An autopsy revealed a small metal pellet near the wound. After analysis, it was found to have contained less than .01 grams of ricin. This tiny amount was more than enough to kill him.

C. Focused response and public health emergencies are two types of incidents which may indicate a biological agent.

1. Focused Response.

A focused response incident involves a single, known point-source of contamination. One example of this would be an individual standing up in a restaurant or theater and announcing that the glass vial in their hand contains anthrax, and then breaks the vial.

2. Public Health Emergency.

The results of spraying salmonella on salad bars in the Northwest is an example of a public health emergency.

D. Potential Bacteria or Rickettsia.

1. Anthrax.

Anthrax is an acute bacteriological disease which can manifest itself as either a skin infection (contagious by direct skin contact only) or in its much more deadly inhalational form. The skin infection starts with a gradual itching and then gradually turns into a depressed lesion which becomes black. This form may turn septic and spread throughout the body via the bloodstream and lymph nodes. Untreated cutaneous anthrax has a fatality rate of 5-20%.

Inhalation of anthrax has two phases. After an incubation period of one to six days, the initial symptoms include malaise, fever, fatigue, non-productive cough, and chest discomfort. The second phase develops suddenly with the development of severe shortness of breath and cyanosis. Shortly after this phase, the terminal phase develops and typically lasts less than 24 hours with a 90-95% fatality rate despite therapy.

2. Plague.

Pneumonic plague is the airborne form of the so-called "black plague". Symptoms include a cough with bloody sputum, fever, and pathogenic (dead) tissue in the lymph nodes. It is rapidly fatal and highly contagious.

3. Tularemia.

Three to five days after exposure to aerosolized Tularemia, there is an abrupt onset of fever, chills, headaches, muscular pain (myalgia), etc., with non-productive cough. It is not considered contagious, but can be fatal.

4. Q fever.

Q fever is caused by a rickettsia-type organism and is rarely contagious. Symptoms include those commonly associated with the flu, acute hepatitis, and pneumonia. Other symptoms are inflammation of the brain and the three membranes or meninges surrounding the brain and spinal cord (meningoencephalitis), inflammation of the membranes surrounding the heart (pericarditis), and inflammation of the myocardium or muscular middle layer of the heart (myocarditis). It is normally not fatal.

E. Potential Viral Agents.

Viruses are different from bacteria in that they grow and reproduce by forcing host cells to produce additional viruses.

1. Smallpox.

Smallpox is infectious as an aerosol. It is highly contagious and has a high mortality rate. After a seven to seventeen day incubation, the pox-like rash starts and patients may present fever, muscle rigidity and shivering, malaise, headaches, vomiting, and other symptoms. Scabs start forming eight to fourteen days after the onset of the disease and leave depressed pigmented scars.

2. Venezuelan Equine Encephalitis (VEE).

VEE is a mildly contagious disease with an incubation period of one to four days. Symptoms usually include fever, headaches, myalgia and vomiting. They may also include drowsiness, chills, sore throat and diarrhea. Can be fatal.

3. Viral Hemorrhagic Fevers (VHF).

Hemorrhagic viruses include Ebola, Yellow Fever, Dengue Fever, Crimean-Congo Hemorrhagic Fever, the Hantaviruses and several others. Symptoms include fever, muscular pain (myalgia), headaches, prostration, hemorrhage, capillary leaks, hypotension, and shock. They are generally moderately contagious and often fatal.

F. Potential Toxins.

Toxic substances are produced by almost every major category of living organism known. Many of the most deadly are produced by fungi, flowering plants and bacteria.

1. Botulinum toxins.

Consists of seven related neurotoxins produced by the *Clostridium botulinum* bacteria. They are some of the most potent toxins known and cause life-threatening paralysis leading to progressive weakness of extremities and respiratory muscles, and ultimately to respiratory failure. Symptoms can occur as early as 24 hours after ingestion.

2. Staphylococcal Enterotoxins.

These toxins commonly cause food poisoning after the toxin is produced in and ingested from improperly handled foods. Inhalation of aerosolized toxin can lead to septic shock and death.

3. Ricin.

Ricin is a water-soluble constituent of castor beans. The wash from preparing castor oil contains up to five percent ricin. As little as a milligram (1/1000 of a gram) can kill an individual. Symptoms from inhalation of ricin include necrotizing (tissue-killing) lesions (injury or abnormality) of upper and lower airway, necrotizing pneumonia and pulmonary edema (accumulation of fluid in the lungs). Symptoms from ingestion or intramuscular injection include gastric bleeding, liver necrosis (death), lymphoid necrosis, splenitis (inflammation of the spleen), and pulmonary congestion.

4. Mycotoxins (Trichothecene Mycotoxins).

These include more than 40 toxins produced by various fungi. Symptoms can include weight loss, vomiting, bloody diarrhea, diffuse hemorrhage, and skin inflammation. Some may cause death.

G. Outward Warning Signs and Detection Clues for the Presence of a Biological Agent.

There are a number of outward warning signs and detection clues which can alert the responder to the possible presence of biological agents both prior to an incident and at the incident scene.

1. Verbal or written threats.
2. Suspicious bombing incidents that do not cause much blast or fire damage.
3. Abandoned spray device out of place for the surrounding environment.
4. Container from laboratory or biological supply houses.
5. Biohazard, culture or culture media labels.

H. Detection methods for biological agents.

On-site detection of biological agents is currently not practical for most first responders. Typically, samples are collected using various techniques including bioassay, mass spectrometry, gas chromatography, and culture of living organisms.

1. Bioassay for Living Organisms and Some Toxins.

Bioassay techniques usually involve taking an unknown sample and comparing its effect on an organism against that of a known substance. Researchers within Army and Navy laboratories are developing assays for botulinum toxin, ricin, plague, brucellosis, Q fever, anthrax, and several viruses.

2. Mass Spectrometer.

Mass spectrometers ionize a sample and then apply electric and magnetic fields to the charged particles (ions). Analysis is derived from measuring the behavior of the ions when exposed to the fields.

3. Chromatographic Analysis of Residue for Toxin.

Chromatographic analysis involves placing an unknown residue in either a single solvent or solvent blend and then comparing the behavior of the dissolved material when subjected to certain pressures and tests against that of known substances. There are several types of chromatography used, involving both liquid and gaseous materials, but all follow the same basic principles. Gas chromatography is often combined with mass spectrometry for a form of analysis called "Mass spec/GC."

I. Proper Self-Protection Techniques.

1. Respiratory Protection

2. Splash Protection (boots and gloves)

3. Emergency Medical Services (EMS) universal precautions including double-gloving.

J. Treatment Procedures for Casualties Should Generally Follow This Sequence:

1. Decontamination;

2. Patient Management;

3. Transport to medical facilities (hospital); and,

4. Definitive care from medical field.

Decontamination covers a broad scope of activities. **Technical Decon** refers to decontamination of tools, suits, and other PPE. **Emergency Decon** of large and small groups - see Section 6, Part D, Appendix 1. **Self Decon** involves a responder who has been contaminated with a hazardous substance. The responder should remove clothing, decon with the appropriate materials, and then cover him or herself prior to seeking medical evaluation. Follow local protocols for detailed instructions.

K. Available Technical Resources.

1. Fire Services - Local and State resources as indicated in the CEMP.
2. U.S. Public Health Service or the Centers for Disease Control.
3. Federal Bureau of Investigation.
4. Department of Defense.

II. NUCLEAR DEVICES**A. Introduction.**

There are three potential forms of nuclear terrorism:

1. Radiological Dispersal Device - Release and dispersal of nuclear materials by packing the nuclear material around a conventional explosive device;
2. Large-scale conventional explosive device detonated in proximity to a target containing large amounts of nuclear materials (power plant or similar facility); and
3. Detonation of a fission device (nuclear bomb).

B. The Radiological Dispersal Device.

Using conventional explosives to spread radioactive contamination is far more likely than an actual nuclear detonation.

In this scenario, radioactive materials are packed around conventional explosives. When the explosive device detonates, it disperses the radioactive material over a wide area. Depending upon the material, both long-term and short-term hazards can be generated with such a device.

Immediate dangers include radiation burns and acute poisoning. Long-term hazards include various forms of cancer and contamination of ground water. This can lead to forced abandonment of large areas or even entire towns.

The New York Times reported that on November 23, 1995, the Russian Independent Television Network was contacted by a Chechan Separatist organization and told of the location of a package in Ismailovsky Park in Moscow. The 30 pound package contained radioactive Cesium (a gamma ray source) and explosives.

One reason that this is a far more likely scenario is that weapons grade fissionable materials are not required for this type of device. Radioactive materials are used in a variety of industrial products, such as radiographic units used to test bridges, buildings, and other structures.

C. Large Scale Conventional Explosion Targeting a Facility Containing Nuclear Materials.

Such facilities include:

1. Military bases where nuclear weapons are housed.
2. Weapons construction / maintenance facilities.
3. Nuclear-powered vessels.
4. Nuclear power plants.
5. Fuel reprocessing facilities.
6. Nuclear waste facilities.

D. Detonation of a fission device.

The third form of possible nuclear terrorism is the least likely. The potential for encountering a nuclear bomb is minimal. Terrorists would find it extremely difficult to build or acquire and use such a device because:

1. In order to build such a device, substantial quantities of weapons-grade fissionable materials are needed. There are three potential sources of fissionable materials:
 - a. Hijacking shipments of spent nuclear fuel;
 - b. Acquisition through black markets; and
 - c. Theft from secured facilities.

Materials acquired from the first two are unlikely to be pure weapons grade and will need further refining, which requires specialized knowledge, skill, money, and equipment.

The largest seizure of weapons-grade Uranium as of 1995 was 2.72 kilograms (about 6 pounds), which should not be enough to build a fission bomb.

Fissionable materials are difficult to transport. A given volume of uranium weighs about 18.7 times as much as water. Therefore, a gallon jug filled with powdered uranium would weigh about 156 lb., not counting the shielding required for safe transport.

2. Building a nuclear device is much more than assembling the requisite quantity of fissionable material. The purified material must be machined into precise shapes and exact quantities of explosives packed around the fissionable material in a geometry that ensures the proper creation of a critical mass for the short time necessary for the reaction to occur. If this is not done, the device will simply scatter the fissionable material over the area instead of detonating.
3. Theft of an operational nuclear device would be even more difficult than acquiring the materials to build one.

Strict global security measures make it very unlikely that an entire bomb could be acquired. Even if such a device was stolen, all western and former Soviet nuclear devices incorporate the Permissible Action Links (PAL) security system which will render the weapons safe unless the correct multi-digit code is entered.

E. Outward Warning Signs and Detection Clues

Outward warning indicators include placards, labels and specialized packaging such as lead containers. Responders should be well-acquainted with the standard radiation warning symbols and hazardous materials containers. For additional information, check the NAERG.

F. Detection Methods for Nuclear Contamination.

Electronic equipment will likely be the only means of testing an area for radiation. Properly trained responders should survey any incident scene with radiation detectors following a suspicious explosion or terrorist threat.

G. Self Protection.

As discussed in Section 6, Part D, Appendix 1, implement personal protection through time, distance and shielding.

H. Treatment Procedures Sequence for Casualties (General):

1. Decontamination.
2. Patient management.
3. Transport to medical facilities (hospital).
4. Definitive care from medical field.

I. Available Technical Resources.

1. County and State Health Department.
2. U.S. Department of Energy (DOE).
3. Federal Bureau of Investigation (FBI).
4. Department of Defense (DOD).

J. Notifications.

Make appropriate notifications as indicated in CEMP.

III. INCENDIARY DEVICES

A. Introduction.

Incendiary devices have been used by terrorists for many years. Fire is a flexible tool that is capable of causing property damage, loss of life, and sparking panic among the public. It will also continue to spread and do damage until all available fuel is consumed, or the fire is extinguished.

In the United States the use of incendiary devices is on the rise.

According to data from the FBI Bomb Data Center:

1. Incendiary devices were used in approximately 20-25% of all bombing incidents in the United States.
2. When used, incendiary devices ignited approximately 75% of the time.
3. Less than 5% of actual or attempted bombings (including those involving incendiaries) were preceded by a threat.

B. Classification of Incendiary Devices.

Incendiary devices can be classified in a number of ways such as by triggering and delivery methods.

1. Classification by Triggering Methodology.
 - a. Chemical reaction (including burning fuse);
 - b. Electronic ignition;
 - c. Mechanical ignition.
2. Classification by Delivery Methodology.
 - a. Stationary (planted);
 - b. Hand-thrown (Molotov Cocktail);
 - c. Self-propelled (rocket, etc...).

C. Components of Incendiary Devices.

1. Ignition source.
2. Combustible filler material.
3. Housing or container to hold the filler.

D. Materials used to construct incendiary devices:

1. Roadway flares.
2. Gasoline and motor oil.
3. Light bulbs.
4. Common electrical components and devices.
5. Matches and other household chemicals.
6. Fireworks.
7. Propane and butane cylinders.
8. Plastic pipes, bottles and cans.

E. Outward Warning Signs and Indicators of Incendiary Use.

These are similar to the detection clues for arson investigations and include:

1. Prior warning (phone calls).
2. Multiple fire locations.
3. Signs of accelerants.
4. Containers from flammable liquids.
5. Splatter patterns indicating a thrown device.
6. Fusing residue.
7. Signs of forced entry to the structure.
8. Common appliances out of place for the environment.

These clues should simply be a signal for the responder to take appropriate precautions to safeguard themselves and the public and to start considering the incident as a potential crime scene.

F. Detection Methods.

Various methods of detecting chemical residue indicating incendiary use are available including: colormetric tubes, combustible gas meters, flame ionization detectors, trained dogs, and photo-ionization detectors.

G. Self Protection.

1. Approach the scene utilizing appropriate personal protective clothing equipment.

2. Do not handle any suspicious device.
3. Avoid vapor clouds, mists, and liquids.
4. Call for technical assistance.

H. Treatment of Casualties.

1. Consider decontamination.
2. Patient management.
3. Transport to medical facilities (hospital).
4. Definitive care from medical professionals.

I. Additional Resources.

1. Local and state resources as indicated in the CEMP.
2. Bureau of Alcohol, Tobacco and Firearms (ATF).
3. Federal Bureau of Investigation (FBI).

IV. CHEMICAL AGENTS

A. Introduction to Chemical Agents.

Chemical agents are substances which can injure or kill through a variety of means. The agents addressed in this section are also identified by military classification codes, which give field personnel a quick reference to their characteristics and hazards. A Persistent Agent is one that remains in the target area for longer periods of time. Hazards from both vapor and liquid may exist for hours, days, or in exceptional cases, weeks, or months after dissemination of the agent. As a general rule, persistent agents' duration will be greater than 12 hours.

1. **Nerve agents** are some of the most toxic known chemicals. They are hazardous in their liquid and vapor states and can cause death within minutes of exposure. Nerve agents, like their close relatives the organophosphorous pesticides, inhibit acetylcholinesterase in tissue, and their effects are caused by the resulting excess acetylcholine.
2. **Vesicants (blister agents)** cause red skin (erythema), blisters, irritation, damage to the eyes, respiratory damage and gastrointestinal effects. Their effect on exposed tissue is somewhat similar to that of a corrosive chemical like lye or a strong acid.
3. **Cyanides or blood agents** include common industrial chemicals such as potassium cyanide, which can cause rapid respiratory arrest and death.

4. **Pulmonary or choking agents** include common industrial chemicals such as chlorine, which can cause eye and airway irritation, dyspnea, chest tightness, and delayed pulmonary edema.
5. **Irritants or riot control chemicals** such as pepper spray cause burning and pain on exposed mucous membranes and skin, eye pain and tearing, burning in the nostrils, respiratory discomfort, and tingling of the exposed skin.

B. Dissemination methods.

1. Aerosol.

An aerosol is defined as a suspension or dispersion of small particles (solid or liquids) in a gaseous medium. Aerosol dissemination methods range from hand-held spray bottles and backpack pesticide spray equipment to powered generators carried by trucks, ships and aircraft.

2. Area contamination.

Area contamination, such as spraying an area with a persistent liquid chemical, can cause thousands of casualties through inhalation or skin absorption.

C. Nerve agents.

1. Examples.

- a. Tabun (GA).
- b. Sarin (GB).
- c. Soman (GD).
- d. Thickened Soman (TGD).
- e. V Agents (VX).

Note: In the military classification of these nerve agents, 'G' refers to German origination and the letter following the 'G' is derived from the name of the scientist primarily responsible for developing that chemical. The letter 'V' stands for 'venom' and the 'X' following the 'V' refers to a chemical series.

2. Exposure and effects.

Exposure to these agents typically occurs through exposure to airborne vapors or direct skin contact with the liquid.

While liquid nerve and blister agents will produce vapors, it is important to understand that they are intended to be aerosolized to maximize their effect. This can be explained in terms of an agent's **vapor pressure**.

The vapor pressure of a substance refers to the relative amount of vapor that will be released from a given substance to reach equilibrium with the liquid or solid form at normal conditions of air pressure and temperature. The higher the vapor pressure, the more vapor will be generated. This, of course, does not take into account such factors as surface area and air currents. Increasing surface area (by aerosolizing) or temperature (by heating, as in a fogger) will increase the amount of vapors generated.

One atmosphere of air pressure is approximately 760 millimeters of mercury (mm/hg). Substances with a vapor pressure at or above this level are gasses. One example is chlorine with vapor pressure of approximately 7,000 mm/hg. Sarin has a vapor pressure of 2.9 mm/hg and that of distilled mustard less than one.

Some nerve agents and vesicants are normally liquids and are classified as Hazard Class 6 by the Department of Transportation. In order to properly weaponize these products, they must be manipulated in a manner designed to maximize vapor release. By aerosolizing them, the terrorist maximizes surface area and provides a maximum amount of vapor and even a means of causing victims to inhale the actual liquid. Heating will also assist in this effort. The sarin used in the Tokyo subway incident was not properly weaponized, which accounts for the limited number of fatalities among the victims.

a. Inhalation Vapors.

A small exposure to vapor can cause pinpoint pupils (miosis), runny nose (rhinorrhea) and mild difficulty breathing.

Large exposure can cause sudden loss of consciousness, convulsions, temporary breathing stoppage (apnea), flaccid paralysis, copious secretions, and death.

b. Liquids on Skin.

Depending on the degree of exposure, symptoms can range from localized sweating, nausea, vomiting, and a feeling of weakness to sudden loss of consciousness, seizures, breathing stoppage, copious secretions, paralysis, and death.

VX is more persistent and harder to decontaminate from the skin than the other agents listed.

3. Outward Warning Signs.

Outward warning signs include observation of symptoms such as miosis, runny noses, difficulty breathing, and uncontrolled muscles and bodily functions. Victims may possibly report a fruity odor.

4. Detection Methods.

a. Detection papers such as M8 or M9;

- b. Colormetric tubes;
 - c. Military detection kits;
 - d. Pesticide tickets; and
 - e. Electronic meters.
5. Self Protection.

Follow agency procedures for operating at the scene of a hazardous materials incident. If the material has not been positively identified but is suspected to be a nerve agent, follow NAERG Guide 153. Do not make entry into confining environments unless you have been appropriately trained and have the necessary equipment. Use time, distance and shielding to your maximum advantage.

Antidotes to nerve agents include Atropine and 2-PAM Chloride.

D. Vesicants (Blister Agents).

1. Examples.
 - a. Mustard (H).
 - b. Distilled Mustard (HD).
 - c. Nitrogen Mustard (HN1, HN2, HN3).
 - d. Lewisite (L).

NOTE: In the classification system devised for the mustard agents, the letter 'H' is derived from the German word for 'hot stuff'. The rest of the letters should be self-evident. Distilled and nitrogen mustards were developed because straight mustard freezes at 50F and is, therefore, unusable in colder climates.

2. Exposure and Effects.

Exposure to vesicants can be through contact with either the liquid or vapor. The warmer the climate, the more easily the vapors are produced.

a. Overview of Effects:

The primary effects of Mustard, Distilled Mustard and Nitrogen Mustards occur in the eye, airways, and skin. Absorbed mustard may produce effects in other bodily systems.

b. Effect on Skin.

Reddening (Erythema) is the mildest and earliest form of skin injury appearing after exposure to mustard. It resembles sunburn and is associated with

itching or a burning, stinging pain. Erythema begins to appear in 2 to 24 hours after vapor exposure.

c. Effects on the Pulmonary System.

The primary airway lesion from mustard is necrosis (death) of the mucosa with later damage to the musculature of the airways if the inhalation exposure is large. The common cause of death in mustard poisoning is respiratory failure.

d. Effects on the Eyes.

The eyes are the organs most sensitive to mustard vapor injury. The time between exposure and visible injury (latent period) is shorter for eye injury than for skin injury.

e. Effect on the Gastrointestinal (GI) tract.

The GI tract is very susceptible to mustard damage, either from systemic absorption or ingestion of the agent.

f. Central Nervous System (CNS) effects.

The CNS effects of mustard remain poorly defined. Animal studies demonstrated that mustards (particularly the nitrogen mustards) are convulsants. There are several human case reports describing people who were heavily exposed experiencing neurological effects just prior to death. Reports from WWI and Iran described people exposed to small amounts of mustard, as appearing sluggish, apathetic, and lethargic.

g. Lewisite.

The effects of Lewisite are similar to that of the mustards, but far more immediate. Lewisite causes immediate pain or irritation of skin and mucous membranes. Delayed symptoms, including erythema and blisters on the skin and eye, as well as airway damage, develop later in a manner similar to that caused by the mustards. To date, there is no documented use of lewisite on humans.

3. Outward Warning Signs.

Outward warning signs include observation of blistering and other external symptoms. Victims may report an odor of garlic.

4. Detection Methods.

- a. Detection papers such as M8 and M9;
- b. Military detection kits;
- c. Colormetric tubes; and

d. Electronic meters.

5. Self Protection.

Follow agency procedures for operating at the scene of a hazardous materials incident. If the material has not been positively identified but vesicants are suspected, follow NAERG Guide 153 as discussed earlier. Do not make entry into confined spaces unless you have been properly trained and have the necessary equipment. Use time, distance and shielding to your maximum advantage.

E. Cyanides (Blood Agents).

1. Examples.

a. Hydrogen Cyanide (AC).

b. Cyanogen Cyanide (CK).

2. Exposure and Effects.

a. Exposure can be through contact with either liquids or vapors. Due to high degree of volatility of these compounds, the liquid rapidly vaporizes and disperses.

b. Hemoglobin carries oxygen to the cells and carbon dioxide back to the lungs for disposal. Cyanides react with the iron in hemoglobin and prevent it from properly taking up and dispensing oxygen and carbon dioxide. The effect is the same as asphyxiation, but more sudden.

c. Symptoms are few. Exposure to high concentration, can lead to seizures, respiratory and cardiac arrest.

3. Outward Warning Signs.

Outward warning signs include victims showing great difficulty in breathing and onset of cardiac symptoms. Some victims may report an odor of bitter or burnt almonds.

4. Detection Methods:

a. Military detection kits.

b. Colormetric tubes.

c. Electronic meters.

5. Self Protection.

a. Follow agency procedures for operating at the scene of a hazardous material incident.

- b. If the substance has been positively identified as Cyanogen Chloride, use NAERG Guide 125.
- c. If the material is positively identified as Hydrogen Cyanide, use NAERG Guide 117.
- d. If a blood agent is suspected, but not positively identified, use NAERG Guide 123.
- e. There is an antidote kit for blood agents called the Pasadena Cyanide Antidote.

F. Pulmonary (Choking) Agents.

1. Examples.

- a. Chlorine (CL).
- b. Phosgene (CG).

2. Exposure and Effects.

Chlorine was the first battlefield gas. It was used by the German army in WWI.

- a. Exposure is through inhalation of vapors.
- b. The primary effect is pulmonary edema. The victim's lungs fill with fluid and they develop severe pneumonia.
- c. Symptoms include eye and airway irritation, dyspnea, chest tightness, and delayed pulmonary edema.

3. Outward Warning Signs.

Outward warning signs include observation of pulmonary distress among victims. They may also report odors such as chlorine, bleach or swimming pool odors (chlorine) and the odor of newly-mown hay or grass (phosgene).

4. Detection Methods.

- a. Military detection kits.
- b. Colormetric tubes.
- c. Electronic meters.

5. Self Protection.

Follow agency procedures for operating at the scene of a hazardous materials incident. If the material has been identified as Chlorine, use NAERG Guide 124.

If the material has been identified as Phosgene, use NAERG Guide 125. If a choking agent is suspected, but has not been positively identified, use NAERG Guide 123.

G. Irritants.

1. Examples.

- a. CS (tear gas).
- b. CR (tear gas).
- c. CN (mace).
- d. OC (pepper spray).

2. Exposure and Effects.

- a. Riot control agents, also called irritants, lacrimators, and tear gas, produce transient discomfort and eye closure to render the recipient temporarily incapable of fighting or resisting. Exposure is through inhalation and absorption of small smoke-like particles suspended in the air. Despite the common names, these are not gasses. They are micro pulverized solids.
- b. Their major activity is to cause pain, burning, or discomfort on exposed mucous membranes and skin; these effects occur within seconds of exposure, but seldom persist more than a few minutes after exposure has ended.

3. Outward Warning Signs.

Outward warning signs include observations of classic 'tear gas' symptoms among victims. They may report multiple odors including hair spray and pepper due the variety of propellants used to dispense these agents.

4. Detection.

There is no detector. The means of identification is by locating and collecting residue for laboratory analysis. Contact state and local law enforcement agencies for additional information.

5. Self Protection.

Follow agency procedures for operating at the scene of a hazardous materials incident. For tear gas or pepper spray, or for unidentified irritants, use NAERG Guide 159.

If Mace is identified, use NAERG Guide 153.

H. Basic Tactical Considerations with Chemical Incidents.

1. **Time** - Keep exposure time and product contact to a minimum.

2. **Distance** - Keep an appropriate distance from the hazardous environment. Stay up wind, uphill, and away from contaminated areas.
3. **Shielding** - Implement appropriate shielding in the form of respiratory protection and protective clothing.
4. Treatment of casualties. Casualty treatment follows a standard sequence:
 1. Decontamination per local protocol;
 2. Patient management;
 3. Transport to medical facilities (hospital); and
 4. Definitive care from medical field.
 5. Additional Resources.
 - a. Local and state resources as indicated in the CEMP.
 - b. The Environmental Protection Agency (EPA).
 - c. The Federal Bureau of Investigation (FBI).
 - d. The Department of Defense (DOD).

V. EXPLOSIVES

A. Introduction.

Bombs appear to be the weapon of choice for terrorists. Approximately 70% of all terrorist incidents involve the use of explosives. Improvised explosives can be designed by terrorists to deliver an assortment of harm and destruction, and can also provide a vehicle for dispersal of chemical, biological, incendiary, and nuclear agents. According to the FBI Bombing Statistics, from 1990 through 1995 there were 10,122 actual bombings (including incendiaries) with another 3,278 additional attempts, resulting in 3,176 injuries and 355 deaths.

B. Terminology.

1. Explosives are defined as materials capable of violent decomposition. This decomposition often takes the form of extremely rapid oxidation (burning). Explosions are the result of sudden and violent release of gas during the decomposition of explosive substances. This release is followed by high temperature, strong shock and loud noise.
2. A common method of classifying explosives is by dividing them according to the speed of their decomposition. While the terms high and low explosive are understood by most people, the correct terminology is high and low order filler materials.

3. When high order fillers are initiated, the reaction is propagated through the filler material at a speed at or above 3,300 feet per second (fps). These explosives are designed to detonate and destroy a target by a shattering effect.
4. When low order fillers are initiated, the reaction is propagated through the filler material at a speed below 3,300 feet per second (fps). These explosives are designed to deflagrate, or burn rapidly, and destroy a target by a pushing and pulling effect.

Both the Oklahoma City and World Trade Center bombings utilized primarily high order fillers to cause maximum damage. The World Trade Center bomb was approximately 1,200 lbs. of Urea Nitrate. The Oklahoma City bomb was approximately 4,800 lbs. of fertilizer grade Ammonia Nitrate and fuel oil. The vehicle bomb used on the barracks in Beirut in 1983 is believed to have contained approximately 12,000 lbs. of explosives which have not been positively identified.

C. Primary Effects of Detonated Explosives:

1. Blast Pressure.

There are two different phases of blast pressure. **Positive blast pressure** (over pressure) moves rapidly away from the explosion center (ground zero) due to the expansion caused by the released energy.

After the positive pressure phase, a **vacuum** is created at the explosion site. This creates a **negative pressure** which moves toward the original center of the detonation at hurricane speed. It is less sudden, but lasts approximately three times as long as the positive pressure wave.

2. Fragmentation.

The explosive device may propel fragments at high speed for long distances. This often accounts for many of the injuries or casualties.

3. Thermal Effects.

Sometimes referred to as the incendiary effect, heat produced by the detonation of either high or low explosives varies according to the ingredient materials. High explosives generate greater temperatures than low explosives; however, the thermal effects from low explosives have a longer duration than high explosives.

The thermal effect is visible in the bright flash or fire ball temporarily produced by an explosion. Thermal effects vary as to type explosive, container, additional fuels/accelerants, shielding, and proximity. Fire and thermal effects are usually localized and short-lived with conventional devices, if they are not enhanced for collateral incendiary effects.

4. Ground Shock.

A fourth effect, ground or seismic shock, is possible, but will usually be generated only by a large detonation. The Oklahoma City explosion, for example, was easily picked up by seismic detection equipment hundreds of miles away from the scene.

D. Types of Improvised Explosive Devices (IEDs) Commonly Used by Terrorists:

1. Vehicle bombs are usually large, powerful devices with a quantity of explosives fitted with a timed or remotely-triggered detonator packed into a car or truck. The two most famous explosions caused by vehicle bombs on United States soil were the World Trade Center bombing in New York and the Alfred P. Murrah Federal Building bombing in Oklahoma City.
2. Pipe bombs are one of the most common explosive devices. They are at the opposite end of the scale from vehicle bombs in terms of size and destructive potential. Pipe bombs usually consist of a quantity of explosives sealed into a length of metal or plastic pipe. Detonation is usually controlled by a timing fuse. Other possible methods include electronic timers, remote triggers, and motion sensors.
3. Satchel devices. The name comes from an old military term for an explosive device consisting of a canvas overpack containing explosives. It was far more powerful than a grenade, but could still be thrown. The container may also be packed with antipersonnel materials such as nails and glass to inflict more casualties. The Centennial Park bombing incident in Atlanta is a clear example of this type device.
4. Other improvised explosives devices may be utilized, including homemade grenades, mines, and/or projectiles.

Explosive projectiles like rocket-propelled grenades, (RPGs) have been used in the past, but have not been a common occurrence. In Fairfax County, VA, police confiscated homemade projectiles capable of exploding on contact, along with tube-type launchers from a private home. This occurred after the individual who had apparently manufactured the devices was found dead in the home. The obvious danger associated with such weapons is the ability of the terrorist to take the threat from a static to a dynamic environment. The possibility of drive-by bombings will certainly increase the operational risk to responders if they are included in the target scenario.

E. Size-up Issues Related to Responder Safety During Operations.

1. Disposition of the Threat on Arrival.

Bombs that are still intact and explosive materials that have not been consumed present extremely dangerous circumstances. The disposition of a bomb threat to the initial responder is a matter of recognizing the presenting hazards such as: has the bomb detonated? If so, is there a concern for dangerous remnants? Are there secondary devices? Etc.

2. Pre-blast or Post-Blast Conditions.

Pre-blast conditions refer to the affected incident environment and/or activities prior to a bomb detonating. This may include a host of activities such as building searches, evacuations, and render-safe procedures. Post-blast conditions refer to the incident environment after a bomb has exploded. This will involve issues dealing with casualties, fires and structural instability to name a few.

3. Explosive Device Size.

The amount and type of ingredients or materials will significantly contribute to the power or strength of the potential blast. Responders should consider size as an element in determining threat levels.

4. Proximity Exposures.

The distance of exposures from the explosive device will likely influence operational objectives such as evacuations, staging locations, medical treatment areas, and perimeter control points.

5. Physical Protection Variables.

Responders should consider using hardened structures such as masonry walls and buildings (not glass), or even fire apparatus to keep responders away from potential line-of-sight blast pathways (remember, stand-off distance significantly factors into selecting physical protection mediums).

6. Condition, Location, Number and Status of Casualties.

When responders arrive at the incident, operational priorities will be influenced by the number and severity of casualties on site. Large numbers of victims may overwhelm initial resources. Also, many types of injuries will require special medical attention. If victims are still trapped beneath rubble, specialized rescue personnel and equipment will be required.

7. Capabilities of Resources On-Hand.

The degree or level of operational involvement of the responders may be predicated upon their training, equipment and in some cases, experience. Responders not trained to conduct *render safe procedures* with explosive devices would be foolish to make any attempt to do so.

8. Reflex/Response Time for Technical Assistance.

Operational decisions will be influenced by the reaction and response time it takes to get specialized resources on the scene. For those responders working a bomb incident located in a rural area, waiting two hours for a bomb disposal team to arrive may not have the same operational impact as it would on responders in the downtown section of a major city.

9. Commitment Level of On-Scene Resources.

Responders should prepare for, and anticipate, difficult decisions early in the response pertaining to the level of operational engagement. For example, the incident commander may elect to commit responders to rescue operations inside an unstable structure, or dedicate responders to assisting evacuees in proximity to an improvised explosive device. Decisions that commit responders to dangerous areas must include the use of a hazard and risk assessment and prescribed (agency) operational procedures.

10. Other Hazards (TRACEM).

Responders should always be aware of the potential for multiple hazards when on the scene of a bombing incident. Explosive devices may have been used to disperse other biological, chemical or nuclear agents.

F. Outward Warning Signs.

Responders must remain alert at all times for warning indicators when involved with suspected bombings. Warning signs include:

1. Any abandoned container out of place for the surroundings.
2. Obvious devices containing blasting caps, timers, booster charges, etc.
3. Abandoned vehicles not clearly belonging in the immediate environment.
4. Strong chemical odors with no apparent reason.
5. Unusual or foreign devices attached to pressurized containers, bulk storage containers or supply pipes.
6. Trip wires or other booby traps.
7. An incident preceded by a written or verbal threat.
8. Suspicious Mailing Containers

G. Detection Methods.

Detection methods are usually limited to outward warning signs for first responders. However, specialized resources will use techniques such as fluoroscopes, detection dogs, and photo ionization detectors.

H. Self protection via Time, Distance and Shielding.

1. **Time** - Work time in the affected area should be kept to a minimum until the area has been evaluated by specialized teams. Teams will search the area for mechanical hazards, unexploded materials, radiological hazards, hazardous chemicals, biological hazards, secondary devices, and booby traps.

2. **Distance** - NAERG Guide 112 provides some guidance when dealing with unexploded materials. It also suggests not permitting radio transmitters (which include cellular phones) within 100 meters (330 feet) of any suspected device.
3. **Shielding** - If practical, keep out-of-line, out-of-sight, of any suspected devices. Buildings and vehicles may provide some protection.

I. Treatment of casualties.

Casualty treatment follows a standard sequence:

1. Decontamination;
2. Patient management;
3. Transport to medical facilities (hospital); and
4. Definitive care from medical field.

Clothing removed from victims may contain evidence that can be recovered. When cutting clothing from individuals, responders should avoid, if possible, cutting through holes in the clothing created by shrapnel or other materials that can yield evidence. Identify and bag all such materials for laboratory analysis.

J. Additional Resources.

1. Local and state resources.
2. Bureau of Alcohol, Tobacco and Firearms (ATF).
3. Federal Department of Defense (DOD).

Appendix 3

Analysis and Response to Threats of Terrorism

This appendix provides a method for addressing threats, making notifications, and taking initial actions during a threat or when an event occurs with no warning.

I. Law Enforcement Response

A. Evolution of Law Enforcement Response to a Terrorism Incident:

Law Enforcement agencies are usually the first responders on the scene of a terrorist incident. This information is included for illustration purposes only. Each situation is unique, as are local conditions and protocols.

II. Receipt of Threat, Initial Local Response

A threat is received at the local, state or federal level. It is assumed that the threat will be conveyed to the appropriate law enforcement agency within that level. It is also assumed that the threat information will be shared between law enforcement agencies at appropriate local, state and federal levels. The first assessment will most probably be made by a local law enforcement agency. Unless that agency has specific information which would discount the credibility of the threat, a response should follow. This may be as simple as consulting with other parties or a physical response to the location threatened. The local law enforcement agency should take actions that they feel are prudent based on their assessment of the threat, the knowledge of the target, etc. This may range from evacuation, negotiation, tactical intervention, explosive ordinance disposal procedures, etc., as dictated by the situation.

III. State Committee on Terrorism

The State Committee on Terrorism (SCOT) has developed a protocol which will enable agencies to call one number - the AEMA Warning Center - to ensure that appropriate state agencies and the FBI are notified of a threat or incident. In addition to such notifications, the SCOT will ensure that appropriate state agencies communicate on a regular basis to enable the most efficient state response.

IV. Initial Federal Actions

If the incident has been identified as a potential terrorist act, and notifications made, the local office of the FBI will initiate a response. This will generally be in proportion to the perceived significance of the threat, and the extent to which the FBI has jurisdiction. The initial FBI point of contact will likely be special agents from a resident agency or field office. FBI headquarters will be advised of the situation, and other federal agencies notified as dictated by the situation. If the initial assessment warrants, the FBI will begin a formal threat assessment process. This involves a joint assessment by experts, combining knowledge of psychological factors, historic and intelligence records, and technical factors such as weapons and methods - all aimed at establishing the credibility of the threat.

enforcement agency and the state. Assuming the threat is deemed credible, the FBI will work with local and state government to begin actions designed to neutralize the threat and/or to deal with its consequences. Depending on the nature and gravity of the threat, this may range from telephone consultation to activation of the county EOC.

Note: Even though these events are typically considered as being within the “crisis phase”, the “consequence phase” planning begins at this point as well.

V. FBI Resources Summoned

If appropriate, additional FBI resources may be summoned. Among those that may become involved in the situation are:

- A. **The Strategic Information and Operations Center (SIOC)** - This is the FBI Headquarters center for command and control, located in Washington DC.
- B. **The Profiling and Behavioral Assessment Unit (PBAU)** - This is a unit at Quantico, Virginia, that develops psychological profiles and assists in the credibility assessment process.
- C. **The Hazardous Materials Response Unit (HMRU)** - This unit is trained and equipped to deal with chemical and biological agents that may be used in a terrorist act or threat.
- D. **The Critical Incident Response Group (CIRG)** - This is an organization at FBI's Quantico facility which includes several units, some of which are listed above. Included is the Crisis Management Unit, which assists local FBI offices in developing procedures and organization to deal with major situations such as terrorist acts. The agency's hostage negotiators are also affiliated with CIRG.
- E. **The Hostage Rescue Team (HRT)** - usually based on the East Coast, is a highly mobile, special weapons and tactics team.

VI. Establishing Joint Operations Center (JOC)

At some point within this time frame, the Federal On-Scene Commander (OSC) will begin the process of establishing a Joint Operations Center (JOC). This is essentially a hybrid EOC/CP which brings together many affected agency and organization representatives. The core operations are primarily composed of FBI personnel (if they have assumed jurisdiction), however there are local, operational area and state representatives included as well. The county EOC will continuously interface and communicate with the JOC, if they are not, in fact, co-located.

Note: In some smaller threats or incidents, local law enforcement (or if appropriate, state law enforcement, i.e., DPS) will retain jurisdiction and control of the entire process, with the federal law enforcement community providing only support and resources.

VII. Threat Executed/Event Occurs

If there is no threat, and an act occurs, most of the steps indicated above occur in more rapid succession - or almost simultaneously. When the event occurs, response is largely dependent on the nature of the act and the dimensions of its impact. ***For a time, crisis and consequence response occur on a simultaneous basis.*** The critical decision must be made whether to turn the location of the event into a crime scene. While lifesaving and life safety are always the pre-eminent considerations, every effort must be made to contain the scene, limit access, and preserve that which remains.

Once the scene is stabilized, law enforcement agencies (federal, local, or a combination thereof) will secure the perimeter(s) of the area. This process will include locating, processing, preserving, and storing the evidence. Human remains may be involved and must be dealt with. These activities may be supported by other entities ranging from the fire service to public works. At some point the crisis phase ceases. Meanwhile, the overall emergency management organization, using the tenets of the Incident Management System, will continue to work to deal with the consequences of the act.

Appendix 4**Department of Defense (DOD) Threat Conditions (THREATCONS)**

The Department of Defense uses the term THREATCONS (Threat Conditions) to describe levels of threats. Military organizations will take certain security actions based upon the THREATCON status. THREATCON levels are usually posted in military installations and are changed (higher or lower) as the situation dictates. The THREATCONS are as follows:

- A. **Threatcon Normal** - No threat of terrorist activity is present.
- B. **Threatcon Alpha** - There is a general threat of possible terrorist activity against installations, building locations, and/or personnel, the nature and extent of which are unpredictable.
- C. **Threatcon Bravo** - There is an increased and more predictable threat of terrorist activity even though no particular target has been identified.
- D. **Threatcon Charlie** - An incident has occurred or intelligence has been received indicating that some form of terrorist action is imminent.
- E. **Threatcon Delta** - A terrorist attack has occurred or intelligence has been received that action against a specific location is likely.

Appendix 5

FBI Threat Levels

FBIHQ has developed a four-level system of describing a developing situation and the thresholds at which particular Federal WMD assets should, in general, be called upon by the SAC to respond to incidents or threat conditions. The Threat Levels are:

I. Threat Level 4: Minimal Threat

Received threats do not warrant actions beyond normal liaison notifications or placing assets or resources on a heightened alert (agencies are operating under normal day-to-day conditions).

II. Threat Level 3: Potential Threat

Intelligence or an articulated threat indicate a potential for a terrorist incident. However, this threat has not yet been assessed as credible.

- A. This should initiate the credibility assessment process.
- B. Notify FBIHQ immediately (WMDOU or SIOC).
- C. As a part of the on-going contingency planning process during the developing crisis, deployment plans for follow-up resources should be made, should they be required.

III. Threat Level 2: Credible Threat

A threat assessment indicates that the potential threat is credible, and confirms the involvement of WMD in the developing terrorist incident. Intelligence will vary with each threat, and will impact the level of the federal response. At this threat level, the situation requires the tailoring of response actions to use federal resources needed to anticipate, prevent, and/or resolve the crisis. The federal response, led by the FBI, will focus on law enforcement actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat. FEMA will support the federal response with consequence management planning and pre-positioning of tailored resources, as required. The threat increases in significance when the presence of an explosive 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 terrorist situation requiring an immediate process to identify, acquire, and plan the use of federal augmentation to state and local authorities in response to the potential consequence of a terrorist use or employment of WMD. At this point, the OSC has the following options:

- A. Deployment of the Domestic Emergency Support Team (DEST) to aid the SAC should it be considered/requested. As the situation develops and warrants, follow-on resources should be requested.

- B. A Joint Operations Center (JOC) should be established to manage the developing crisis in the interagency environment incorporating law enforcement planning concerns with consequence management concerns.

IV. Threat Level 1: WMD Incident

A WMD terrorism incident has occurred which requires an immediate process to identify, acquire, and plan the use of federal augmentation to state and local authorities in response to limited or major consequences of a terrorist use or employment of WMD. This incident has resulted in mass casualties. The federal response is primarily directed toward public safety and welfare and the preservation of human life.

- A. FEMA would lead the federal government's efforts to respond to the devastation through consequence management in support of the FBI as the Lead Federal Agency (LFA).
- B. A Joint Operations Center (JOC) should be formed to integrate consequence management concerns with the law enforcement effort. The perpetrators may have additional devices. The investigation should continue under the JOC command concept until the threat of additional devices is mitigated or other contingencies regarding the incident are resolved. The incident site may expand to multiple sites which can be strategically coordinated by the JOC.
- C. All chemical, biological, or nuclear material should be approached by authorized personnel only, which includes the Hazardous Materials Response Unit (HMRU) and/or Technical Escort Unit (with HMRU coordination).
- D. No untrained field agent should inspect known or suspected chemical, biological, or nuclear materials. Field testing and transportation for lab testing is to be coordinated with HMRU.

Appendix 6

Threat Data Elements

I. Threat Report Elements

The following data elements are suggestions. They are not all inclusive. Many agencies have very complete and sophisticated threat reporting, analysis, and notification systems. These data elements are offered:

- A. To provide a minimum, common baseline database.
- B. To provide jurisdictions without existing systems a point of departure for development of their own threat reporting, analysis, and notification systems.

Data elements to consider when taking an initial report:

- 1. Report date/time
- 2. Report received by (name, organization, and phone number or EMAIL).
- 3. Threat transmitted by (telephone, fax, EMAIL, video, mail, other).
- 4. Type of threat (bomb, chemical, biological, radiological, "cyberterrorism", hostage situation, other).
- 5. Description of threat.
 - a. Content of threat.
 - b. Characteristics of threat (describe caller, describe FAX, describe EMAIL, describe video, describe mail, etc.).
 - (1) Target(s) of threat (specified or potential based upon data)
 - (2) Timelines (when is the event going to occur?).
 - (3) Brief initial assessment of threat.
 - (4) Other agencies/organizations notified of threat.
 - (5) Has any individual, group, or organization claimed responsibility for threat/event?

II. THREAT ANALYSIS

Data elements to consider during threat analysis for a threat analysis report.

- A. Technical feasibility (Is this threat technically feasible?).

1. Technical analysis prepared by (organization).
- B. Operational practicality (Is the threat operationally possible to accomplish?)
 1. Operational feasibility analysis prepared by (organization)
- C. Behavioral resolve (Do the potential terrorist have the resolve, moral support, or behavior profile?)
 1. Behavior analysis prepared by (organization)
- D. Final analysis/conclusion (Is the threat credible? If so, why? If not, why not?)
 1. Final analysis/conclusion prepared by (organization)
 2. Date/time of report

III. NOTIFICATION ACTIONS

Data elements to consider for notification.

- A. Date/time of Notification
- B. Notification made by (agency/individual name)
- C. Summary of threat (who, what, when, how, why)
- D. Summary of threat analysis (conclusion and agency making analysis)
- E. Recommended courses of action
 1. Agencies to notify
 2. EOCs or Command Post Activations (federal, state, local, private organizations/businesses)
 3. Possible response resources required (law enforcement, fire and rescue, medical, public works, etc.)
- F. Report received by (organization/name)

APPENDIX 7

Unified Command and Incident Management

I. Purpose and Scope

This document clarifies how local, state, and federal agencies can successfully manage emergency incidents through the application of unified command at the field level.

II. General Concept

A. The Response Structure

State and local agencies use the Incident Command System (ICS) as the structure to manage emergency incidents at the field level. ICS incorporates the concept of unified command when more than one agency is responsible for the emergency incident. This system allows agencies to exercise their responsibilities without compromising jurisdictional authorities.

There are four elements to consider when applying unified command:

1. Policies, Objectives, Strategies

The responsibility to set joint policies, objectives, and strategies for an incident belongs to the various jurisdictional and agency administrators who set policy and are accountable to their agencies. This activity is performed in advance of tactical operations and may be coordinated from a location other than where the field response is taking place.

2. Representatives

The unified command organization consists of the on-scene senior representatives (agency incident commanders) from the various agencies with responsibility for the incident.

3. Resources

Unified command resources are the personnel and equipment supplied by the jurisdictions and agencies that have responsibility for the incident.

4. Operations

Unified command resources stay under the administrative and policy control of their agencies; however, operationally, resources are deployed by a single Operations Sections Chief based on the requirements of the consolidated action plan. Consolidated action plans identify objectives and strategy determinations for the incident made by the unified command. The incident objectives must adequately reflect the needs of all the jurisdictional agencies.

Unified command represents an important element in increasing the effectiveness of response to multi-jurisdictional or multi-agency incidents. As incidents become more complex and involve more agencies, the need for unified command is increased.

B. Interagency Agreements

Agencies that will be partners in a unified command situation should, whenever possible, establish agreements in advance of emergency incidents that identify jurisdictional and functional responsibilities and delineate the elements of the unified command structure. In addition, agencies should take every opportunity to exercise the provisions of these agreements through periodic training and simulation drills.

C. Incident Management Applied - Coordinating Diverse Authorities

A cornerstone of incident management is the application of ICS in emergency incident management at the field level. Under this system, unified command must be used when emergency incidents involve multiple agencies and/or jurisdictions. The basic precept of unified command is that all agencies with jurisdictional responsibility for the incident will manage an incident by establishing a common set of incident objectives and strategies. This is accomplished without losing or abdicating agency authority, autonomy, responsibility or accountability. Therefore, in order for federal, state and local agencies to be consistent with incident management, the unified command must include all the individual authorities with response jurisdiction over the incident.

NOTE: Any process used by the unified command must permit the command team to develop a consolidated action plan that adequately reflects the jurisdictional needs of the agencies with responsibility for the incident. Unified command is based on the presumption that all responsible agencies will cooperate in a collective effort to mitigate an incident.

D. Recommendations For “Best Practices”

When addressing pre-existing mandates within incident management, the following guidelines should be applied.

1. Incident management must be viewed as a structural system only, not a preemption authority.

Incident management is an emergency response management structure designed to focus resources and effort in the most efficient fashion. It is an “overlay” to pre-existing mandates in statute and regulation. It does not re-direct or preempt these authorities.

2. Jurisdictional authorities must not be compromised.

A basic precept of unified command is that jurisdictional authorities responsible for the incident are never excluded from the command structure. The legal requirements for federal, state, and local agencies must be taken into account when developing a consolidated action plan. Exactly how those jurisdictional authorities function in the unified command is a matter to be determined according to the details of the incident and the parties involved.

3. Jurisdictional mandates must be applied within incident management in a flexible manner.

Incident management is meant to be flexible and applicable to many disciplines involving many agencies. There will almost always be overlapping authorities subject to interpretation. Federal, state, and local agencies must coordinate with each other in applying and exercising their respective authorities within the unified command. Individual agencies do not exercise jurisdiction or authority that exceeds their legal limits or usurp the authority of another agency—there is no “vote” inside the unified command. It is incumbent upon the agencies involved to cooperate in order to allow for a successful resolution to a complicated emergency response organizational issue. Often, these issues can be dealt with through pre-planning.

4. Pre-planning and training must be continuous.

It is essential to the success of efficient emergency management that jurisdictions and functional agencies pre-establish the unified command structure and conduct frequent drills to exercise the system.

5. Cooperation and consensus must be a priority.

It is impossible to implement unified command unless the responsible agencies have agreed to participate in the process. Once this has been achieved, incident management goals, objectives and strategies are established through a consensus process.

6. Establishment of the unified command structure must be expedited.

Implement unified command promptly when it is needed in a multi-jurisdictional or multi-agency incident. It is essential to begin joint planning as early as possible, especially on those incidents where there may be conflicting priorities based on agency responsibilities. Initially the participants should: identify statutory authorities for all agencies; determine a clear functional structure for the incident; coordinate initial activities; and open clear communication channels at all levels of the organization. Conversely, individual agencies in the unified command should not exit the response structure until their jurisdictional responsibilities have been resolved and an orderly transition has been orchestrated.

7. Proper integration into the ICS structure is essential.

A member of the unified command is very different than an agency representative. The unified command consists of agencies with direct jurisdictional responsibility for the incident. Agency representatives are individuals assigned to an incident from assisting or cooperating agencies. Agency representatives are personnel other than those on direct tactical assignments or those involved in a unified command.

III. Summary

Incident management provides the structure for managing the response to multi-agency and multi-jurisdiction emergencies and facilitates coordination among all responding agencies. ICS provides a flexible structure at the field level for coordination of response activities which is geared to the needs of a specific incident. Unified command allows agencies that have responsibility for an incident to meet their statutory requirements through a coordinated process involving diverse jurisdictional authorities.

Blank Intentionally