Appendix S

Response to Terrorism Plan

EXECUTIVE SUMMARY

This document is intended to provide guidance to support agencies during a terrorist event. It identifies lead personnel and a plan of action. It is not intended to replace existing first responder operation procedures, but serves as a guide to terrorist attack and threat response management for events involving Weapons of Mass Destruction. It presents planning guidelines for local emergency management, law enforcement, fire rescue, and emergency medical/health services response.

The Eagle County Office of Emergency Management, in its role as the County's emergency management agency, is implementing a systems approach for a unified response to a terrorist event. This approach is designed to complement the State of Colorado and Federal Terrorism Response Plan Annexes. Additionally, this document facilitates the escalation from local first response to the more definite federal response. This document, in conjunction with the Eagle County Emergency Operations Plan constitutes a coordinated and integrated approach to these types of events. It must be emphasized that the key component of success is a unified management approach.

PURPOSE

To protect persons and property from the effects of terrorist acts, and provide guidance to primary responders and support agencies in the event of a terrorist act.

INTRODUCTION

The U.S. Code of Federal Regulations defines terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives".

Conventional terrorist attack utilizes bombs, bullets, and weapons such as knives, grenades, etc. Unconventional terrorist attack use the unexpected, such as, using vehicles as weapons, gases, biologic agents, chemicals, stolen nuclear weapons and other weapons of mass destruction, etc.

Terrorist incidents involving chemical, biological, radiological, nuclear or explosive materials (CBRNE) are considered weapons of mass destruction (WMD) events.

Incidents, which are believed to be terrorist acts, will be treated as a hazardous material incident with additional complicating factors.

The Federal Bureau of Investigation (FBI) further describes terrorism as either domestic or international. These distinctions are based on the origin, base and objectives of the terrorist organization involved. Further definitions of these two types of terrorism are:

- Domestic terrorism involves groups or individuals that are based and operate entirely within the United States and Puerto Rico. They do not receive foreign direction and their acts are directed at elements of the U.S. Government or population.
- International terrorism is the unlawful use of force or violence committed by a group or individual having some connection to a foreign power or whose activities transcend national boundaries.

EXAMPLES OF TYPES OF TERRORIST ACTIVITIES

Armed Assaults - Armed assaults can include a wide variety of direct action. Examples include throwing hand grenades into crowds or rocket attacks on airlines or buildings. Another type of increasingly familiar example involves routine traffic stops that evolve into armed confrontation(s) between police and extremist militia members.

Arson - Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires a low level of technical knowledge.

Assassination - A term generally applied to the killing of prominent persons and symbolic enemies as well as traitors who defect from the group. Assassination targets are generally selected carefully with a strategic purpose, and the actual attack is planned, coordinated and practiced.

Biological Agent Release - Biological agents consist of organisms or chemicals of biological origin that cause death and disease among humans, animals and plants. Biological agents include anthrax, cholera, plague, botulism and ricin among others.

Bomb - Bombs can range from very simple to extremely complex. They can consist of ounces of explosive packaged in letter bombs, to tons of explosives in a large vehicle bomb. A burning time fuse can initiate a bomb, a sophisticated electronic time delays mechanism or can be booby-trapped, and detonating when disturbed. Bombs have been incorporated in letters, packages briefcases, computers, purses, luggage and automobiles. Although bombs overwhelmingly remain the weapon of choice for terrorists, it must be realized that others may use this technique as well. Revenge, extortion, mischief and vandalism by neighbors, former lovers, juveniles or co-workers have all been cause for bombing(s).

The improvised explosive device (IED) is the contemporary terrorist’s weapon of choice. An IED is inexpensive to produce, and because of the various denotation techniques available, is a low risk to the perpetrator.

Bomb Threat – Any terrorist group that has established credibility can employ a hoax with considerable success. A bomb threat can close a commercial building, empty a theater, or delay an aircraft flight at no cost to the terrorist. Bombs threats are a close relation to actual bombings. Most bombings are not preceded by a telephone message or written threat, but bomb threats cannot simply be ignored. Bomb threats can cost schools and businesses considerable loss of productivity if a bomb incident management plan is not developed and implemented.

Chemical Releases - Of the five categories of chemical agents (nerve, blister, choking, blood and vomiting), nerve gas is undoubtedly the most notorious and dangerous. Terrorist use of a chemical agent in a closed environment such as a subway station (i.e. Sarin used in the Tokyo subway system) auditorium, sports arena or shopping mall has the potential for creating mass casualties.

Civil Disturbance - A large, often violent public demonstration intended to attract media coverage that will help convince the world that the event organizers represent a popular cause.

Cyber Terrorism - Terrorists can use sophisticated hacker skills remotely to enter computer systems in order to steal funds, or alter information in databases and operating systems. Cyber terrorists may also attempt to gain control of, or disable, critical facility infrastructure components such as dams, utilities or airport radar systems. This increasingly costly tactic is emerging and may be used by terrorists in with increasing frequency.

Environmental Destruction - Examples would be the intentional dumping of hazardous chemicals into a city's water supply or the destruction of an oil tanker.

Hijacking or Skyjacking - Hijacking is normally carried out to produce a hostage situation and to gain media attention to the hijacker's cause. Aircraft are the preferred target, because of their greater mobility and vulnerability.

Hostage Taking - This 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(s). 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.

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 who are held until specific demands are met. Kidnapping for ransom is becoming an increasingly favored method of financing terrorist operations in parts of the world.

Nuclear Weapons/Devices - The nuclear terrorist threat consists of improvised nuclear devices (IND) capable of creating a nuclear yield and radiological dispersion devices (RDD) (sometimes referred to as "dirty bombs"). INDs include nuclear weapons obtained from a nuclear

power inventory, or improvised devices designed and constructed by the terrorists. RDDs employ conventional explosive devices to distribute radioactive material, contaminating a wide area.

Product Tampering, Sabotage - Sabotage of industrial or commercial facilities is one means of identifying the target while making a statement of future intent. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and gains immediate public attention.

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 to facilitate logistic purposes (i.e. robbery of a bank or armory).

Seizure - This 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.

CYBERTERRORISM DEFINITIONS

Activism – Normal, non-disruptive use of the Internet in support of an agenda or cause.

Hacktivism – Operations that use hacking techniques (system infiltration, mass e-mail, computer viruses, etc.), to attack a computer system, company, or other user. It commonly results in denial of service or theft of information.

Cyberterrorism – Politically motivated attack against information, computer systems, computer programs, and data intended to cause harm, such as loss of life or severe economic damage, for furtherance of political or social objectives.

- The susceptibility of computers and their networks to those with criminal intent is well documented and publicized. From the security of individual e-mail, to incidents of hackers gaining access to Department of Defense systems, the need for ever-increasing and evolving computer security is obvious. However, the ability of recognized terrorist groups to achieve the goal of inflicting casualties on a civilian population via the Internet is somewhat more questionable.

PREVENTION

Cyber terrorism techniques are continuously evolving so no single preventative measure will be effective. It is reasonable to consider that security measures already utilized by those responsible for operating computer networks can and must continually evolve to keep up with the threat of cyber criminals.

ASSUMPTIONS

- Targets (hard and soft) exist in Eagle County
- Law enforcement organizations can, with cooperation, protect the public
- Terrorist elements exist
- Alert police and security forces may block attempted terrorist acts
- Individuals are responsible for taking reasonable precautions for their own defense/protection
- Attacks may be conventional or unconventional
- Procedures are in place for those injured by a terrorist act
- There is a possibility of secondary devices aimed at responders

Both crisis management (law enforcement) and consequence management (emergency management) will be occurring simultaneously with crisis management in the lead until a transition to consequence management is coordinated.

No single agency at the local, state, federal or private level possesses the authority and expertise to act unilaterally on issues that may arise in response to threats or acts of terrorism.

Local, state and federal responders may define working perimeters that may overlap to some degree. Perimeters may be used to control access to the area and assess potential effects on the population and the environment. Control of these perimeters may be enforced by different authorities, which may impede the overall response if adequate coordination is not established.

An act of terrorism, particularly an act directed against a large population center within the United States involving CBRNE/WMD, may produce major consequences that would overwhelm the capabilities of many local governments almost immediately. Major consequences involving CBRNE/WMD may overwhelm existing state and federal capabilities as well.

If protective capabilities are not available, responders cannot be required to put their lives at risk in order to enter an area contaminated with CBRNE agents. It is possible that the area will be closed until the effects of the CBRNE material have degraded to safe levels or properly trained and equipped responders are available.

RISK ANALYSIS

The Eagle County Office of Emergency Management (OEM) has identified numerous possible terrorist targets. The Eagle County Threat Hazard Identification and Risk Assessment identifies these locations and is an Official Use Only document.

CONCEPT OF OPERATIONS

Initial Notification - Those first aware of a terrorist situation in any jurisdiction should call 911. The Public Safety Answering Point (PSAP) will notify the appropriate law enforcement agency and other emergency response agencies as necessary.

First Arriving Units - First arriving units (police and fire) will establish an exclusion zone around the area or suspected areas(s). If necessary, and safety permitting, an on-scene command post will be established nearby. Traffic will be re-routed around the exclusion zone.

Law Enforcement Protocols -Existing protocols (radio/telephone procedures, equipment, methods of operation, transportation, etc.) will be used during all counter-terrorist operations.

Lead Agencies - During a federal crime, the federal agencies will be Lead Agencies requiring state and local assistance.

Local and State Agencies - Local and state agencies must work closely together and coordinate their activities to assist federal agencies during terrorist incidents.

Shelters - Temporary shelter(s) will be opened in accordance with Eagle County EOP, Appendix G, for those affected by the incident and unable to return to their residence.

Joint Terrorism Task Force (JTTF) - A JTTF, or working group, will be established. JTTF will consist of federal, state, and local law enforcement agencies, emergency management personnel, and the Governor's staff, if required. The JTTF will be responsible for determining protective actions, such as evacuations, increased security, planning, training, etc.

Incident Command System (ICS) - ICS will be utilized by all agencies involved. Unified Command will be necessary because of the different jurisdictions/disciplines involved.

ROLES AND RESPONSIBILITIES

Office of Emergency Management - In the event of a major or catastrophic emergency event the Eagle County OEM will activate the Emergency Operations Center (EOC) to support the initial response, recovery and provide consequence management.

FBI - According to Homeland Security Presidential Directive -5, "The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 and other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive Order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the

activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States."

Local Law Enforcement Agencies - It is likely that Law Enforcement agencies will be among the event's first responders. The agency having jurisdiction (AHJ) will be lead response agency. AHJ supports police, security, and law enforcement operations, and coordinates with other law enforcement organizations during terrorism incidents. Law enforcement agencies if required are responsible for the scene security, traffic control and subsequent incident investigation. Support from other Law Enforcement agencies or Emergency Services (if necessary), may include: bomb squad; K-9 units; Haz Mat teams; hostage negotiators; and homicide investigations. Law enforcement may be required to provide security and crowd control at various locations, including shelters, medical facilities, casualty collection points, etc. As soon as it has been determined that an event indicates terrorist activity, the FBI will become the lead response agency.

Fire/Rescue/Emergency Medical Services - Eagle County Emergency Medical Services, Fire and Rescue agencies are responsible for the life safety issues relative to an incident involving terrorist act. They may be the first, or among the first, incident responders. These agencies are responsible for fire suppression, victim extraction, decontamination, immediate treatment, triage, and patient transport. Specialized teams (HAZMAT or Search and Rescue) may be requested to assist, if necessary.

Hospitals - Area hospitals will, most likely, receive the brunt of casualties (victims) affected by the terrorist act. Medical facilities must be prepared for triage, decontamination and treatment of victims. Many will leave the incident area before the arrival of first responders, and transport themselves into the medical facility, placing hospitals and medical providers at risk of cross-contamination. The affected jurisdiction PSAP will be responsible for prompt notification of all area medical facilities

Eagle County Public Health and Environment - It is the responsibility of Public Health and Environment to collect information, monitor local trends and notify the Centers for Disease Control if necessary, and to maintain a connection with medical providers for notification of reportable diseases and trends surveillance.

Eagle County Coroner - The Coroner is responsible for the investigation and process of any fatalities, possibly with outside assistance. Any fatalities due to a terrorist act are considered murder victims; therefore, the location should be cordoned off and the area secured as a crime scene. Everything within the crime scene is considered evidence and should not be disturbed, except by investigators and/or specialized law enforcement personnel.

Continuity of Government - Eagle County is governed by a Board of County Commissioners (BoCC). During times of Emergency the County Manager is given the authority to accomplish actions necessary to protect lives. The authority succession is:

County Manager ➡ Deputy County Manager ➡ Chair of the BoCC

Continuity of Government (COG) is an essential function of governmental agencies at all levels and is vital during an emergency/disaster situation. COG is defined as the preservation, maintenance, or reconstitution of the civil government's ability to carry out its statutory responsibilities. Consequently, if a unit of government is not prepared, most if not all of its critical governance ability could be severely degraded. Such a situation could create a climate that could make the jurisdiction vulnerability to anarchy, lawlessness, and chaos. The resources of all County and Municipal governmental departments and agencies are considered to be available at the County and/or Municipal level in minimizing the effects of disaster; these resources will be supplemented, as determined by necessity and availability, by voluntary assistance from:

- Adjoining counties
- Private businesses and industry
- All other groups and individuals

Once activated, Eagle County Emergency Management will coordinate county resources for prevention, preparedness, response, recovery and mitigation operations through the EOC.

All agencies countywide should have established lines of succession in the event their key individuals are unavailable.

Any additional assistance required at any level will be requested through the EOC.

During a terrorist incident, all unaffected government offices and organizations should continue to operate with increased security until notified otherwise. Increased security includes individual employee awareness, observation, reporting of suspicious objects and characters (see something/say something), the immediate challenge of all suspicious persons, places or things foreign to the normal business environment and any prudent method to secure the facility and protect its occupants.

Administration and Logistics - Each agency, office, and/or organization involved is responsible for its own administration and logistics. Detailed logs, financial records and receipts are to be kept for possible future reimbursement and possible legal proceedings. These logs and records shall be submitted to Eagle County OEM upon request.

Each local agency is responsible for maintaining a list of emergency resources to include private resources, personnel, supplies and equipment. The EOC shall prepare situation reports (which will also be submitted to the State Division of Homeland Security and Emergency Management) and After Action reports describing the situation and response actions of local, state, Federal agencies and private sectors.

REGIONAL RESPONSE ASSETS

Eagle County has mutual aid agreements in place should outside assistance be required.

MITIGATION AND PREVENTION

Reducing the Risk - Terrorism prevention begins with the local community and facilities. There are warnings that, if noticed, can indicate potential terrorist activity. Police, fire, public works and the general public need to know what potential indicators are and have a system to report suspicious activity. Public and government sectors need to acknowledge the potential threat and implement physical security programs commensurate with the threat and value of facilities to be protected. The terrorist's greatest asset is anonymity and the ability to reach his potential target unnoticed. Mitigation (prevention) actions are meant to thwart the potential terrorist and reduce the probability of an incident. Communities, agencies, facilities and individuals can reduce the risk of becoming terrorist targets by understanding the nature of terrorism, assessing their risk, and by taking basic systematic security precautions.

PHYSICAL SECURITY

Physical security measures for a facility reduce the probability for terrorist attack by making the act more difficult for the terrorist. Developing its defensive capabilities enhances the security of any public facility. Employing an integrated system of intrusion detection equipment, barriers, structural hardening, access control and trained response forces are critical components of this defense, as is delaying terrorist action until additional forces can arrive. Measures designed to prevent unauthorized access to facilities, equipment, material and information will also safeguard against sabotage, vandalism and theft.

Awareness Education and Training - The key element to an effective anti-terrorism program is to develop awareness.

MONITORING

Law Enforcement agencies, in particular the FBI and the Colorado Information Analysis Center (CIAC), will monitor known groups or factions which are suspected of, or who have the potential to commit terrorist acts. Local law enforcement will be alerted to treats in our area.

TRAINING

It is the responsibility of local agencies and departments to provide all appropriate training.

Eagle County OEM will provide training information and/or materials from the various sources and will facilitate training as necessary. Training session information (and such) will be announced, as it becomes available. Each organization should determine the level of training for their personnel.

ALERT AND NOTIFICATION AND ACTIVATION LEVELS

Alert and notification will encompass of the following:

- Threat information assessment and initiation of protective measures
- Notification of appropriate agencies who will be responding or will be placed on stand-by in the event of terrorist actions

On-Scene Warnings are situations that are observed on-site which would indicate something out of ordinary, such as:

- Unexplained illnesses or deaths
- Items that seem out of place – unattended packages, suitcases, containers, bulky envelopes, etc.

SECONDARY DEVICES

In terrorism incidents, always consider that a secondary device is present. This will prevent unnecessary casualties/fatalities. Bomb Squad or other qualified personnel should make determination of secondary devices. Keep potential consequences of secondary devices in mind when organizing the response site and executing the response. Establish functional areas as far away from the incident as practical. These include the Incident Command Post, staging area(s), triage/treatment area (s) and decontamination site(s). Cellular phones, radios, pagers and car alarm remotes must be turned off or kept away from suspected bombs. Radio frequency transmitted by one of these devices could cause device detonation.

RECOVERY

Long-term activities stabilize all systems. The length of the response will depend on the type of incident. The most complicated recovery period would be if the incident involved nuclear, biological or chemical agents. Issues to consider are:

- Extent/Degree of allowable re-entry
- Extent of chemical, biological and/or nuclear contamination
- Identification of agents

- Identification of contaminated victims
- Identification of contaminated facilities/sites
- Decontamination effort
- Quarantine activities
- Identification of successfully decontaminated facilities/sites
- Identification of "lost" facilities/sites (those which cannot be safely decontaminated and are determined unsafe for future use)
- Economic impact