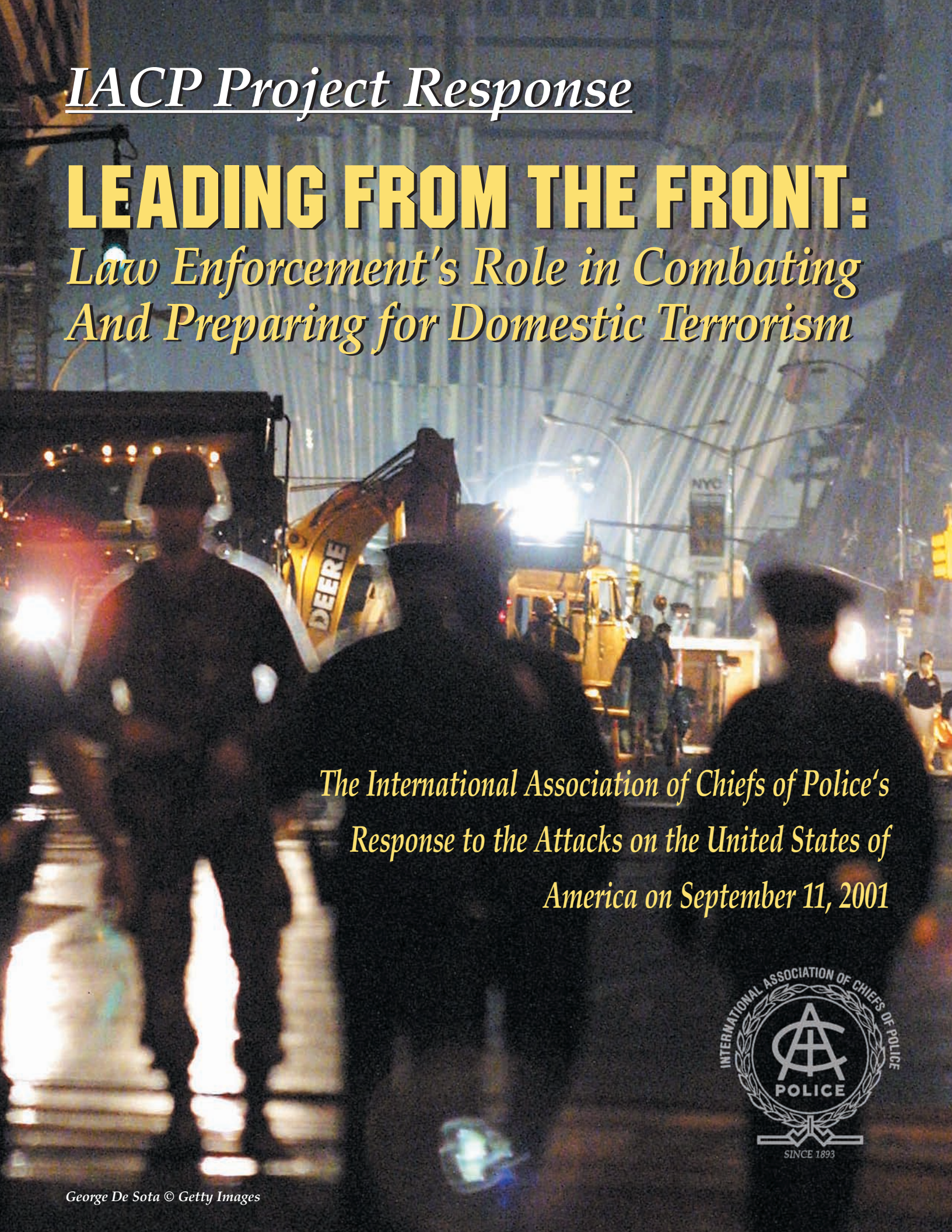
IACP Project Response

LEADING FROM THE FRONT:

Law Enforcement's Role in Combating And Preparing for Domestic Terrorism



The International Association of Chiefs of Police's Response to the Attacks on the United States of America on September 11, 2001

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
POLICE
SINCE 1893

George De Sota © Getty Images

Bruce Glasscock	President
Daniel N. Rosenblatt	Executive Director
Eugene R. Cromartie	Deputy Executive Director

Project Response Team:

Charles Higginbotham
Project Response Director

Robert Rowe
Project Response Manager

Joe Bui
Marcie Deitch
John Firman
Larry Haynes
Jennifer Hicks
Jerome Needle
Erin O'Brien
Anthony Pizarro
Matt Snyder
Katherine Spivey
Dave Tollett
Nancy Turner
Gregg Walker
Jennifer Wykoff

Contributing Writers:

Jeff Beatty
Total Security Services International

Thomas Brandon
Deputy Inspector
Suffolk County, New York, Police Department

Pat Devlin
Assistant Chief of Police
New York City, New York, Police Department

Edward Flynn
Chief of Police
Arlington County, Virginia, Police Department

Audrey L. Honig
Director of Bureau Operations
Employee Support Services Bureau
Los Angeles County, California, Sheriff's Department

Robert D. MacLean
Sergeant
U.S. Park Police

Donald McLellan
Lieutenant
Oakland County, Michigan, Sheriff's Department

Dave Mulholland
Lieutenant
U.S. Park Police

Daniel J. Oates
Chief of Police
Ann Arbor, Michigan, Police Department

Donald Pike
Lieutenant (Retired)
Gaithersburg, Maryland, Police Department

Joseph Polisar
Chief of Police
Garden Grove, California, Police Department
IACP Third Vice President

Jack Van Steenberg
Major
New York State Police

Dedicated to men and women of the police departments and all others who answered the call on September 11, 2001, and paid with their lives.

International Association of Chiefs of Police
515 N. Washington St.
Alexandria, VA 22314
703-836-6767; 1-800-THE IACP
Fax: 703-836-4543
www.theiacp.org

Preface

The following Project Response is IACP's attempt to delineate the steps that law enforcement leaders need to take to strengthen their effective response to ongoing terrorist activity.

No place can be made entirely immune from terrorism. We in the United States learned that in Oklahoma City in 1995; we learned it again on September 11, 2001, with the attacks on the World Trade Center buildings, the Pentagon, and the hijacked plane in Pennsylvania.

This Project Response is a starting point. It gives you the questions you must answer—you are, after all, the expert in your own neighborhood, your own community. You alone know the most vulnerable targets you need to protect, as well as the people and groups you need to protect—the people looking to you for leadership.

Realistically, the United States of America—and the world, for this report can be applied to any locale facing the threat of terrorism—covers a huge variety of terrain and population density. No one document could address each locale in enough detail to be useful without being cumbersome.

In addition, we cannot adequately address all the intelligence responses and systems in this document, since legislation is currently being proposed in the U.S. Congress that will change the face of U.S. intelligence gathering. However, we are aware of the need for intelligence sharing among federal, state, and local agencies—as well as international groups—and the need for centralization. Our legislative effort, concentrated in the United States, will be directed toward making intelligence gathering easier for law enforcement.

A complete overview of all processes and elements may not be available for many months and will involve much more information than can be presented here. Therefore, this *Project Response* will be a living document, updated as more information is revealed. The document will be available on the IACP website, http://www.theiacp.org.

Table of Contents

Introduction

On September 11, 2001, everything changed.

On September 11, 2001, the theoretical became real. International terrorists killed thousands of people by flying commercial passenger airliners into and destroying several of the World Trade Center buildings in New York City, heavily damaging the Pentagon and killing personnel there, and killing passengers on an aborted airliner that crashed near Shanksville, Pennsylvania.

While these acts occurred in the United States, citizens of many nations were victims in the attack. At the time of this publication, it is known that the United Kingdom, France, Japan, and Israel—as well as many other countries—lost citizens in these attacks.

In response to these attacks, the largest criminal investigation ever conducted is underway; military actions against terrorist strongholds are being taken; and new procedures, legislation, and laws are being prepared. However, while we strengthen our efforts to thwart future terrorist attacks, democratic nations must maintain their founding principles of freedom, civil liberties, and individual rights. The investigation and response—more than any other before it—will be a balancing act of pursuing intelligence leads and adhering to the policies that protect our cherished individual rights.

No matter how the future unfolds, local law enforcement will be on the front lines. In democratic societies, an enormous degree of responsibility and authority for public security is historically delegated to the local government, particularly to police agencies. As the September 11, 2001, attacks show, the local police will often be the first responders to any and all incidents.

Primary Goal

The primary goal of law enforcement is to ensure public safety. Even just the threat of terrorism can undermine that safety since it is often not the actual physical harm that can send a community into disarray but citizen perception of danger. Local police leadership is urgently needed. A police chief must act to allay those emotions and concerns. Regardless of where an incident occurs, the confidence and ability a chief imparts regarding the response to and control of the situation in his or her community will affect how safe citizens feel and how normally they live their lives.

The material presented here first discusses what every chief should know about weapons of mass destruction (WMD) that terrorists are likely to use. The next sections chronologically set out an overview of critical elements that need attention at the three stages of an event: before, during, and after an incident.

Weapons of Mass Destruction (WMD)

At present, the three types of weapons most commonly categorized as WMD are nuclear weapons, biological weapons, and chemical weapons. Subcategories of WMD include agroterrorism and cyberterrorism.

The potential use of chemical, biological, radiological, and explosive devices as terrorist tools exists. As deadly as explosives, firearms, and incendiary agents can be, the destructive capabilities of nuclear, biological, and chemical (collectively NBC) weapons are many times more formidable. WMDs are, by definition, weapons that have destructive capabilities far in excess of conventional weapons such as explosives, firearms, or incendiary agents. WMDs can not only cause extensive casualties and damage to infrastructure at the point of impact, but disrupt services for communities far from the site of the attack. Citizens everywhere may experience adverse psychological effects.

Nuclear Weapons

Terrorists may choose between two different types of nuclear attack: (1) a nuclear explosion, as produced by an atomic bomb, or (2) the dispersion of dangerous radioactive materials throughout the target location.

Nuclear bombs may be difficult to recognize visually, because these devices may take a number of different forms, which can be concealed in many varieties of packaging. Improvised nuclear devices can be made to fit into the trunk of an automobile or an ordinary shipping crate. The automobile, crate, or other housing could then be left in the desired location and detonated by a timing device, radio signal, anti-tampering mechanism, or other method.

Less spectacular than a nuclear bomb explosion—but potentially just as deadly—is an attack by dispersion of radioactive material in a targeted area. Different types of radioactive materials could be employed and might be in particulate, liquid, or other form. Without scientific equipment and expert assistance, recognizing these radioactive materials is virtually impossible.

Radioactive substances can be dispersed in many ways, including introduction into water supplies of communities or targeted businesses through the building's ventilating systems. One of the more effective means involves using an explosive radiological dispersion device (RDD) to spread particulate radioactive materials throughout the target area. These RDD devices can easily be fabricated from common, locally available materials such as ammonium nitrate and blasting caps. The dispersion of the material into the atmosphere can be accomplished either by the RDD explosion itself, or for greater effect, by placing the device on or near a source of combustion such as a large gasoline or propane stor-

age tank. The exact degree of dispersion would be determined by wind speed, wind direction, and other atmospheric conditions existing at the time of the event.

Biological Weapons

The biological warfare threat is greatly magnified by the urban and suburban nature of today's society and the increasing availability of biological weapons to those who desire to use them. This last factor is particularly disturbing, for biological agents are now obtainable by terrorist groups through countries that support terrorism, or even through domestic sources from which biological material can be procured either openly or taken by violence or subterfuge.

There are numerous biological agents that could be employed by terrorists. The US Army Medical Research Institute of Infectious Diseases lists the following diseases and biological toxins as potentially suitable for introduction into the population by deliberate dispersal:

1. ***Bacterial infections.*** These include anthrax, cholera, plague, tularemia, and "Q" fever.
2. ***Viruses.*** Included here are smallpox, Venezuelan equine encephalitis, and viral hemorrhagic fevers.
3. ***Biological toxins.*** These include botulinum, staphylococcal enterotoxin B, ricin, and T-2 Mycotoxins.

Biological agents may be difficult or impossible for police or other emergency personnel to recognize by mere appearance, since the biological organisms are microscopic in size and may be easily disguised in media such as harmless—appearing liquids. Even after the biological agents have been dispersed and symptoms have begun to appear, specialized medical equipment and expertise are required to positively identify the specific agent involved.

There are many ways to deliver biological agents to a target area. They could be put in the public water supply or introduced into ventilating systems in large buildings or, in the larger cities, the subway systems. In other areas the biological agent could be dispersed into the air by aircraft over the target area. For example, freeze-dried anthrax spores could be placed in pressurized metal containers equipped with aerosol release valves and hidden in air distribution vents at the target location. The release valves would be designed to release the spores at a time when the maximum number of people are present such as during country fairs, outdoor athletic events, and tourists spots during peak holiday seasons. By this means, millions of the disease organisms could be spread throughout the target location.

The exact effects of the biological agent will, of course, depend upon the agent used. In general, effects of biological agents will be felt only after an incubation period lasting up to several days. For example, anthrax has an incubation period of one to six days. In its early stages, anthrax produces flu-like symptoms: fever, malaise, fatigue, cough, and mild chest discomfort. Severe respiratory distress and cardiac problems may follow these initial effects. Shock and death may occur within 24-36 hours of the onset of severe symptoms.

Chemical Weapons

A variety of chemical agents can be acquired and used by terrorists. Unlike the nuclear and biological agents, which have limited actual past use as offensive weapons, many of the existing chemical agents have been used in warfare. Among the commonly employed chemical agents are the following:

1. ***Nerve agents.*** One of the better known of the nerve agents is sarin (GB), which was used in the Tokyo subway attack. As the generic name suggests, all of these agents incapacitate or kill by attacking the nervous system.
2. ***Vesicants.*** The most familiar of these is probably mustard (HD, H), often referred to as "mustard gas." Lewisite (L) is also a vesicant. The vesicants are so named because, among other unpleasant results, they cause blistering of the skin.
3. ***Lung-damaging agents.*** Most prominent among these is phosgene.
4. ***Cyanide.*** This is a highly lethal agent but one that is not always well suited to terrorist use because it dissipates quickly.
5. ***Riot-control agents.*** Among these are CS and CN, both of which are familiar to law enforcement officers. Although these are, technically, chemical agents, because of their normally non-lethal effects they are less likely to be the agent of choice in a terrorist attack than the other substances referred to above.

Prior to their actual release into the population, nerve agents are difficult to recognize by methods other than scientific analysis, since they may appear in solid, liquid, or gaseous form. By contrast, vesicants such as mustard (HD, H) sometimes can be identified without specialized equipment. Mustard may appear as an oily liquid, ranging in color from light yellow to brown. However, it does vaporize, and the vapor hazard increases with temperature. Mustard usually emits an odor of garlic, onion, or mustard (hence its name), but odor cannot be relied on for detection. Chemical agents used in an attack can often be tentatively identified by the nature of the symptoms that they cause.

Chemical agents can be dispersed as solids, liquids, gases, aerosols, or vapor. They may therefore be delivered in a large variety of ways. For example, they may be packaged in pressurized metal vessels with aerosol release valves and introduced into a ventilating system, or they may be hidden in bulk somewhere in the target area, such as in lockers, waste bins, or the like, and dispersed solely by natural vaporization.

It is also possible to deliver chemical agents through the use of bombs, shells, missiles, or mines; all disperse the chemical upon detonation. For terrorist purposes, planting a bomb containing chemical agents could easily be accomplished. For example, the bomb could be concealed in a package, suitcase, knapsack, or other container that can be left in an appropriate location without arousing suspicion, such as a baggage claim area or locker. With this type of delivery, the detonation of the bomb serves not only to disperse the chemical agent, but also to cause damage and casualties from the force of the explosion, thus making this approach doubly attractive to terrorists.

It may also be possible to deliver chemical agents by overflying the target area, although this method is usually not ideal for terrorist purposes because it is often difficult to obtain the concentration necessary to make a chemical attack effective.

The effects suffered by the victims of a chemical terrorist attack will vary depending upon the type of agent used and other circumstances. Many of the nerve agents—which, because of the success of the 1995 Aum Shinrikyo sarin gas attack on the Tokyo subway system—demonstrate the need to guard against chemical threats. Sarin typically produces blurred vision, pain in the eyes, tightness in the chest, vomiting, dizziness, and disorientation. Heavy exposure may produce copious bodily secretions, convulsions, loss of consciousness, cardiac symptoms, paralysis, and, ultimately, death. Mustard, another chemical agent terrorists are likely to use, produces skin blisters, eye injury including blindness, respiratory distress and damage, gas-

trointestinal effects, and other adverse physiological results.

Agroterrorism

An attack against agriculture, livestock, or other food supply is referred to as agroterrorism. Consumer product and food tampering came to the national front in the 1980s when a significant attack against a food supply occurred in Dalles, Oregon. Followers of the Bagwan Shree Rajneessh cult sprayed salmonella on salad bars in several area restaurants, causing 751 people to become ill. The future potential of such attacks requires local law enforcement and public health agencies to continuously improve coordination and readiness.

Cyberterrorism

Terrorists believe that countries such as the United States rely too much on communication and information systems and they plan to exploit this alleged weakness. The potential of disseminating viruses, launching denial of service (DOS) attacks, disrupting e-mail servers and disabling websites, as well as hacking into basic infrastructure systems such as electric power, telecommunications, banking and finance, gas and oil, and transportation systems, creates a whole new list of vulnerabilities subject to theft, alteration, or destruction.

I. BEFORE AN INCIDENT: PLANNING AND PREPARING

While billions of dollars will, and should, be spent on federal-level preparedness and response to terrorism, one fact remains clear: the first responders to these acts will be beat cops—and they will need the leadership of their chiefs to do the right job.

—Chief Ed Flynn, Arlington County, Virginia, Police Department, On-Scene Response and Security, Pentagon Terrorist Attack

Leadership in planning and preparation before an incident occurs highlights the ongoing responsibilities of police chiefs. In dealing with the possibilities of terrorist attacks and incidents especially where WMDs may be used, chiefs and other law enforcement executives should implement the following steps along with the items explained more fully in this report:

- Develop pertinent policy
- Implement procedures
- Train personnel
- Rehearse possible events
- Acquire equipment
- Establish mutual-aid agreements and multijurisdictional protocols
- Establish multidiscipline community service teams

A well-maintained and -trained department will be prepared to respond to any type of situation and implement with skill and efficiency the policies and procedures that are in place, thus saving lives, maintaining safety, and calming fears—the true goal of the front line of any emergency situation.

Information Is Power

To both prepare for and respond to a terrorist threat or attack, police chiefs throughout the world have many intelligence opportunities available. Part of any chief's preparation should include thinking strategically about how to gather and process intelligence. Here are some key areas where police chiefs can obtain critical information to avert or prevent an incident through intelligence sources:

Access Law Enforcement Information Databases

The best prevention against terrorist acts at the local and state level is to maintain an ongoing intelligence-gathering and -coordinating enterprise with state and federal agencies. In particular, the counterterrorist activities of the Federal Bureau of Investigation (FBI) and intelligence-gathering operations of the Bureau of Alcohol, Tobacco, and Firearms (ATF) are essential resources for state and local law enforcement agencies. They should be used both to receive intelligence information and to provide and coordinate intelligence information. Other intelligence-gathering information systems and related criminal investigation databases cannot be overlooked and should be used whenever possible. Important among these are the Regional Information Sharing Systems and the El Paso Intelligence Center (EPIC), which is a cooperative effort staffed by personnel from 14 federal enforcement agencies. EPIC has information-sharing agreements with all 50 states and can be used by any state or local law enforcement agency.

Reach Out to All Federal Sources

While the FBI is the designated lead counterterrorism agency in the United States, police chiefs must also build and maintain strong ties and an open dialogue with other federal law enforcement agencies. Chiefs should establish local meetings as an opportunity to build these relationships. There is no substitute for personal contact among high-ranking law enforcement officials. Chiefs should work to create and maintain strong personal relationships at the high-command level, sharing home phone numbers, cell phone numbers, and 24-hour contact numbers. Chiefs should, in calm times, work hard to build these relationships, developing trust and opening strong lines of communication. In times of crisis, chiefs can make immediate contact with counterparts and talk often enough to ensure that everybody is on the same page about the emergency.

Network with Local Chiefs

Similar to the federal source recommendations outlined above, neighboring chiefs have their own skilled officers, intelligence networks, and sources. In times of crisis, they will be dealing with their own worries. Yet all local chiefs offer tremendous potential to each other, as long as they talk. Just as with the federal agencies, dialogue among local chiefs (including state police commanders and other state and regional law enforcement heads) will naturally lead to a sharing of information.

Critically Assess Every Unusual Event

Chiefs should watch for unusual incidents, even seemingly unimportant ones. Depending upon the terrorism threat or crisis, the possible link to an unusual local event may be obvious. In times of crisis, however, anything out of the ordinary cannot be dismissed. Responding officers, witnesses, and potential subjects should be closely questioned and the information passed on appropriately. A very practical tool to ensure that this is done is to keep a running log, 24 hours a day, of all unusual events. This way, even if the immediate staff handling the incident does not perceive its intelligence value, senior staffs' later review of the log may pick up on the opportunity and justify further investigation.

Participate in Intelligence Clearinghouses

The best method to ensure that information is shared and intelligence opportunities are exploited to their full potential in a crisis is by using regional intelligence centers. The best of these typically involve the joining of personnel and databases from all of local law enforcement (often with federal agencies participating) under the same roof. Police

organizations should link up to existing intelligence centers such the High-Intensity Drug Threat Area or El Paso Intelligence Center, which provide 24-hour clearinghouse for information.

The point of contact can be as straightforward as the desk officer, duty command officer, or dispatch center in a selected centrally located police department. The point is to have one place those local chiefs and their staff can call to report and share tips, leads, and information. Better still, if resources permit, is to have people from several agencies analyzing the incoming information for its intelligence value.

Community Assessment: Locating and Measuring Risk

Reducing a community's vulnerability to attack requires, among other things, analyzing a locality to identify likely targets and working to improve the security at these locations. Completely protecting every reservoir, parking garage, mass transit terminal, large building, and other likely targets within a jurisdiction is not possible. However, the more difficult it is for terrorists to introduce weapons into a given area or facility, the less likely they are to initiate an attack.

The chief's first step to assess community risk is to assign an officer or unit to identify potential targets and to enhance security at those targets. This step must be taken even when a department's resources are limited. In preparing a community plan, the officer should assess potential targets, consider security measures, help develop a security plan for potential targets, and advise on protective measures.

Many entities have developed a rating system and sorted their problem areas into different priority levels. A typical system has four levels: fatal, critical, important, and routine. Using the functions within a police department illustrates how risk can be assessed in the community.

First Priority Level—Fatal: Functions whose failure could result in death, severe financial loss, or legal liability to the department. It includes all essential (mission-critical) functions in the operation of information systems and delivery of services to community and department staff. Examples include E911 systems, telecommunications equipment, and two-way radios.

Second Priority Level—Critical: Functions that are critical to department operations and difficult to do without for any length of time. Examples include PCs for data entry, security systems (badge readers), elevators, and programmable thermostats.

Third Priority Level—Important: Functions that are not critical to the agency. Examples include copiers, fax machines, and still and video cameras.

Fourth Priority Level—Routine: Functions that are not strategically important to the department and whose failure would inconvenience individuals but not disrupt projects. Examples include automatic coffeepots, VCRs, and microwaves.

Evaluation should be ongoing, and assessments should be made not only on the basis of routine operation and testing, but also on the efficacy of the procedures should an actual attempt occur.

Police chiefs should constantly maintain and update a list of a jurisdiction's critical assets and vulnerable infrastructure points. During the planning stage, law enforcement officials must examine the potential targets and vulnerable locations in or near their jurisdiction. An inventory of locations where large crowds assemble, high-profile locations, transportation facilities, symbolic sites, and other targets of opportunity should be developed and maintained. Primary attention should be given to water sources, waste treatment facilities, international businesses, financial institutions, major utilities, communications centers, university research laboratories, schools, town halls, post offices, courthouses, police departments, and other government buildings. This inventory must be checked and updated regularly.

After identifying the targets, law enforcement leaders should try to get a sense of the weapons or objects in their jurisdiction that could be used as weapons including the presence of materials that may be employed by those seeking to develop a WMD. Locations that have toxic industrial chemicals, conduct biological research, or utilize explosives are prime candidates. Chiefs should consider how each weapon might be used against each target, and what law enforcement responses to that threat should be. This brainstorming will help police prioritize their limited resources and identify things for which they will need more help from the community.

The people who work at these facilities are also a great intelligence resource. They should be instructed on the nature of the threat and asked to act as the eyes and ears of law enforcement. Seemingly innocent but unusual events in and around a critical infrastructure point may, upon analysis, suggest that the site has been studied as a possible target for terrorist action. The best source of intelligence is often law-abiding citizens who notice—and report—unusual activity occurring around them.

The following list is designed to help chiefs identify areas at risk in their communities and anticipate possible issues:

- ***Public utilities (electric, water, natural gas, waste treatment):*** Have emergency systems been tested? Are they ready? Is there a contingency plan? Are alternative sources of water available?
- ***Fire departments:*** Do they have contingency plans? Have they considered the possibility of more fires if citizens use alternative sources of heat? Will sufficient vehicle fuel be available? Are gas pumps compliant? Are generators available?
- ***Grocery stores:*** Are cash registers and inventory control systems ready? If not, will stores be open? How will they operate?
- ***Banks:*** Are banks ready with extra cash?

This evaluation process may appear overwhelming, but smaller agencies can begin by doing a walk-through of their agency. Larger agencies can delegate the evaluations to their subordinate commands. No one is in a crisis alone: businesses, governments, and even residences will be similarly affected.

An agency review may provide insights into communications, utilities, and so on, but may not typically address the public works department, for instance. This oversight can have far-reaching implications. For example, localized power outages call for manual traffic direction in intersections controlled by electrical devices. Also, if such events require increased staffing, there will be a corresponding increase in the need for food and fuel. Local food or gas suppliers could run short, requiring alternative sources. All these external considerations should be factored into your assessment and contingency planning.

Using the Media to Reach the Community

During an incident such as a terrorist attack, whether it occurs in the immediate jurisdiction or thousands of miles away, a law enforcement executive must release information to the local community as accurately and as quickly as possible. A policy and established mechanism for releasing information will facilitate the necessary community response for

public safety, alleviate unnecessary fears and panicked responses, and reassure the community that its public safety agencies are well prepared and are executing an efficient response. The media provides the most efficient means to rapidly inform the community of the incident and the ensuing response.

The foundation for effective communication to the community through the media begins with a strong, open media relations program, which should have started before the crisis. A partnership approach to law enforcement and media relationships is crucial. The law enforcement executive must understand that the media play a dual role during a critical incident: to obtain information and footage of the incident for news reporting purposes, and to quickly and efficiently notify the community of impending danger, identify appropriate reactions, and provide reassurances. A good media relations program includes a plan to supply information to the public during a critical incident.

Established agency incident response plans should include procedures for communicating with and through the media. These plans must be developed in conjunction with local media representatives, not solely by the law enforcement agency. Roundtable and practical exercises to prepare for incident response should include media participation, as it would in real life. These exercises present opportunities for dialogue with the media to discuss what information can and should be released and to explain why certain information cannot be immediately released.

Finally, strategic media events should be staged to continuously inform the public that the agency is well trained, well equipped, and well prepared to handle a critical incident. When new equipment is obtained or incident response training occurs, the media should be invited. These events should be well publicized to let the community know that the agency is aware of the possibility of incidents and is constantly preparing for such an event. Again, this relationship should not have to be created at the time of the crisis.

Voice and Data Communications: The Critical Link

If an agency waits until a critical incident occurs to consider how it will manage voice and data communications during that time, the odds of failure are greatly magnified. The importance of robust, redundant, and scalable communications solutions cannot be overemphasized. After each major event in recent history, the most glaring indication of success or failure by responding agencies has been their ability to effectively communicate with each other.

Critical incidents do not know jurisdictional boundaries. Chiefs must think about how their agencies will communicate during a critical incident with the following agencies:

- Fire Services
- Emergency Medical Services
- Public Works
- Departments of Transportation (local and state)
- Neighboring and concurrent jurisdiction public safety resources (local, state, federal)

Planning

All communications systems should be inventoried, serviced, and tested on a regular basis. When the critical incident occurs, leaders should know what is on hand, where it is located, who can operate it, and the process to follow to keep the system operational. A sufficient supply of serviceable batteries should be available to allow for long-term operations. A system should be in place to distribute and recharge those batteries during the course of an incident. Protocol on securing alternate sources of energy, such as generators, should be known in advance and include plans to connect, activate, and fuel them.

Ideally, a system should be in place to maximize inter- and intra-agency communication. Efficient methods of communications must exist among police, fire, EMS, public works, transportation, and other critical incident assets. But interoperability should also go beyond jurisdictional boundaries by including neighboring jurisdictions and state and federal resources.

While this concept is far from being realized in most jurisdictions, planning and preparation stages are the perfect stages to consider how an incident commander or police supervisor in the field would access and communicate immediate needs to any other asset available on the critical incident team. If the process requires an officer to call a dispatcher who in turn telephones another dispatcher, the dispatchers obviously need to know how to contact each individual agency.

Ideally, communications systems would have a redundant fail-safe backup. If such a backup is in place, it should be tested regularly so that during crises the transition is immediate and flawless. If a redundant system is not available, chiefs should identify logical backups. For example, a mobile data computer system with messaging capability may serve as a backup to a failed voice communications system. A cellular telephone network may serve as a backup to failed Land Mobile Radio Systems (LMRS) voice or data communications services. Also, one- and two-way paging systems may be able to replace or supplement other methods of communication.

When purchasing a mobile computer or voice communications system, the vendor should address contingency and interoperability plans. If the system is already in place, law enforcement and communications officials should ask the system's vendors to examine the existing system and identify backup and contingency plans should a critical incident occur. Some mobile radio systems can be programmed to function in a fail-safe mode, while others can include universal emergency frequencies that permit cross-jurisdictional communications.

Alternative communications solutions must be identified in advance, and procedures must allow smooth transitions. All parties using a particular communications system should know what the backups are and how to transition from one to another during a critical incident.

When considering the physical security of the communication and information technology resources, the following locations need to be surveyed:

- Dispatch centers (primary and alternate)
- Command posts
- Antenna sites
- First-responder facilities
- Information technology facilities

Key data on department information systems should be backed up on a regular basis and stored in a separate, secure, and fortified site. Keeping computer backups in the same facility that stores the original data is useless in the event of any disaster, whether natural or man-made. The data that should be backed up include computer-aided dispatch data, records management system data, evidence and property data, personnel data, e-mail data, and other critical data found on servers and desktop computers. A system is required in order to regularly conduct backups and secure the saved data. The system administrator should also have a plan for collecting automated data when servers are temporarily down as well as a plan for restoring systems that have been destroyed utilizing stored data and original program files.

Incident Management Plan

To address a crisis efficiently is to have thought it out beforehand and properly planned for it. With planning, much of the chaotic activity usually produced by these kinds of events can be avoided. To ensure the plan is uniformly understood and acknowledged, the elements must be known. Historically, the response to critical incidents shows that there is a direct link between planning to include practicing response plans and the quality of the response to an actual critical event.

Through planning and exercising, participating agencies can ensure the broadest access to and use of resources, as well as minimal duplication of effort.

Pre-incident Planning and Exercising

An incident management plan must be made operational, which includes training personnel and installing any required systems or protective devices. Periodic testing and drills must be conducted to demonstrate security preparedness. The procedures should be frequently reviewed and revised as necessary.

Both the Federal Emergency Management Agency (FEMA) and state emergency management agencies require communities to examine the risks they face, from such incidents as technological emergencies involving radiological or hazardous materials releases or major aircraft crashes, and natural disasters such as floods, tornadoes, earthquakes, and hurricanes. After completing these hazard analysis studies, each community is expected to prepare response plans for the expected hazards. Response plans identify authority levels and responsibilities, determine resource needs and access, and identify mutual-aid protocols. Incorporating responses to potential bombings or other forms of terrorist attacks can also be accomplished in these plans. Once the plan is written, it must be exercised and updated annually.

Exercises

The follow-up to plan development is to test the plan by conducting multidisciplinary exercises based on a community's assessed risks. Those communities that have conducted pre-incident exercises based on well-developed community response plans and have actually faced critical incidents have discovered that planning and exercising substantially improved their personnel's performance. Exercises work out relationships and problems before an incident occurs.

Chiefs should consider an often-neglected area in their exercises and include victim services representatives in the planning and testing response protocols. Besides including the victim-centered crisis response teams in the exercises, assistance can be obtained from victim services and mental health programs to train officers in:

- understanding the crisis/trauma reaction, including the causes, compassion fatigue, and acts of aggression or hate
- obtaining information from victims and witnesses in shock
- understanding their own reactions
- coordinating with local or national crisis response groups

Lessons learned also illustrate the need for the department to assess the number of personnel with children and what childcare problems may result from a sustained activation of long-term shifts. It may be necessary to establish some creative childcare assistance back-up plans for the personnel involved in the crisis.

Updating the Response Plan

Communities change over time. Businesses come and go. Neighborhoods and highway systems change as well. A community's response plan must be routinely updated to ensure it contains current information. A chief may want to include several critical planning steps. The following list contains the most significant areas of concern:

Contingency Planning Checklist

- Identify priority or principal targets for attack
- Establish protocols on who will be in charge on-scene (incident command)
- Establish inner and outer perimeters with appropriate staff access to and through each
- Establish predetermined response routes to locations
- Establish emergency command center and backup/redundant center
- Check communications interoperability with other first responders (fire/EMS)
- Stockpile emergency equipment/ supplies
- Disseminate attack response plan document (formal report)
- Hold mock disasters to test response plan
- Establish lines of communication with the following offices:
  - -FEMA
  - -The state emergency coordinator
  - -The city/county emergency coordinator
  - -Emergency coordinators in neighboring jurisdictions
  - -The Red Cross
- Establish memoranda of understanding (MOUs) with neighboring jurisdictions for the purpose of sharing information and resources
- Designate shelters in the event of power outages and/or loss of heat (Develop a plan for heating the shelters)
- Develop a plan for directing traffic
- Develop a plan for food and water distribution
- Develop a plan for crowd control and civil unrest
- Formulate a contingency plan for problems affecting transit
- Make the public know and understand what to do in case of emergency
- Plan on your department's delivering a consistent message to the community
- Prepare to have enough dispatchers and police personnel to meet additional needs
- Be aware of unique personnel needs that could result from sustained activation of long-term shifts
- Set up victim-centered crisis response team to develop protocol for on-scene crisis response for victims and witnesses

Gathering Resources

In an emergency, the public looks to law enforcement to respond and mobilize staff, equipment, and resources to deal with it. While law enforcement may not always be the lead agency in some situations involving natural and manmade disasters (though they are often the first responders), law enforcement officers still play a very important role in mitigating further damage and injury. Since many agencies respond to emergencies and natural and manmade disasters, the effort must be integrated and coordinated. To ensure that response is adequate to meet a variety of needs, and to ensure an appropriate provision of service, all members from responding law enforcement agencies—sworn and nonsworn—must be familiar with the components of their respective agency's emergency and contingency plans, personnel mobilization procedures, and available resources.

Regardless of size or mission, all law enforcement agencies should have comprehensive plans that take into account a variety of contingencies and available government and community resources. For smaller agencies—the kind that rely heavily on larger county or state agencies for assistance—the plan may be written from the perspective of a first responder to provide guidance to officers until additional help and resources arrive or a

county or state emergency plan is activated.

While predicting emergencies and disasters is impossible, planning for such events is essential. Components of a comprehensive plan include:

Food

During pre-incident planning, chiefs should identify sources of food in the community and where, how, and by whom the food should be acquired, stored, and served. While no law enforcement agency is responsible for acquiring, storing, or serving this food, law enforcement agencies must identity the capabilities of stores, religious facilities, community service organizations, charities, and government and nongovernment agencies. Food and potable water raise concerns because of the shelf life of some foods, the need to refrigerate others, and the need to ensure the safety of water for human consumption. This is especially significant in the event of a chemical or biological attack on a waterway, reservoir, or water system. In most cases, bottled water in sufficient quantity should address the problem.

During this planning process, the law enforcement agency must also consider the provision of food and water for its on-duty personnel. For agencies whose jurisdictions include a water system or a waterway or reservoir that is a source of drinking water, agencies should consider the level of security to be assigned these facilities.

Shelter

Planning agencies should identify those facilities that will be used as shelters both inside and outside the agency's jurisdiction. In some jurisdictions, high schools are considered prime shelter locations because they can accommodate a large number of people, are ADA compliant, and have showers and other facilities. The plan may also identify those instances when in-place sheltering may be preferential to a full-scale evacuation and relocation. This is significant for those agencies that have hospital(s) or other in-patient health care facilities—some of which may contain immobile patients—in their respective jurisdictions. After shelters have been identified, law enforcement agency plans should identify the means by which persons will reach them. For safety and security reasons, shelters must be properly staffed. Agencies must consider whether a law enforcement or security officer needs to be assigned to each facility.

Emergency Aid

In pre-incident planning, agencies should consider the various types of aid that are available inside and outside the jurisdiction attacked. Even though laws may govern mutual aid during emergencies, solid and comprehensive written agreements should be executed long before they are needed so providers and receivers know what is expected of them. Since fire service and EMS personnel will most likely be the next responders after police and the lead agency for the incident, they must plan a coordinated response and consider a unified command post, staging areas for responding fire apparatus not yet needed at the scene, and capabilities and limitations. Other emergency aid to be planned for and mobilized may include animal control officers, American Red Cross, and the National Guard.

Vehicles

Agencies should consider all types of vehicles. How many buses are available and from what source? What types of special-purpose vehicles, such as boats, four-wheel-drives and SWAT vehicles, are available to law enforcement? What types of vehicles will be used to transport prisoners?

Planning at the pre-incident and during-incident levels should take into account how certain vehicles will be used, staged, or parked, and the access to inner and outer perimeters. Maintaining security of the vehicles is also important. If police vehicles are equipped with in-car video cameras, determining how and where those vehicles are deployed could be important.

Commercial and government owned vehicles, such as dump trucks, front-end loaders, tractors, should be included in the vehicle plan. They can come into service in cleaning debris from roadways.

Civilian Assistance

Individual civilians and civilian groups can provide assistance in the time of crisis. At the pre-incident level, planning should identify those individuals in the community who have technical skills or expertise in a given field that might be useful in an emergency. Also, planners should also compile a list of bilingual persons, especially those who speak the languages most prevalent in the community, and those who know sign language. In addition, some civilians are amateur radio operators who can be especially helpful in the event of a failure of a public safety radio system or when the responders need to enhance existing communications.

Protecting Our People: Addressing Backlash

A resulting danger of a terrorist attack is the hate-crime backlash attacks on community members who share the race, ethnicity, or other characteristics of the group accused of the attack. As such, chiefs should expect reports of harassing calls, hate mail, graffiti, verbal abuse, and maybe civil disobedience; they should also be prepared for incidents of physical assaults and batteries, arsons, drive-by shootings, bombings, riots, and even murder.

Community policing can be a strong asset here. Chiefs must have built partnerships with their communities, especially those segments that are on the margins or that have historically been disenfranchised. Chiefs should know the leaders in these segments and develop a rapport with those from the faith, the business, and the activist communities. These relationships do not form overnight, and it takes a genuine commitment on the chief's part to create and cultivate these relationships.

Chiefs must ensure their officers have had the most up-to-date training available in cultural awareness and hate crimes, which should reflect the diversity of the community's ethnic and religious groups. Officers should also have mobile field force and crowd-control training to handle potential demonstrations or civil disobedience. Chiefs of smaller agencies in the same area should encourage their departments to train together to form a multiagency team.

Finally, chiefs must ensure that their officers are equipped with the tools necessary to protect every citizen in their community. Should people pose a threat to minority citizens, accessibility to the latest in less-than-lethal technology such as bean bags, tasers, and pepper spray is critical. Officers should have gas masks for their own protection.

II. DURING AN INCIDENT: EXECUTING AND RESPONDING

On-Scene Command Leadership

The police are nearly always going to be the primary responders to the scene of any catastrophe, including a terrorist attack. Their first priority is to protect the public and secure the scene. Upon arrival, these first responders (usually uniform beat officers) must assess the situation and begin initial response activities.

Many challenges await the chief at the scene. The chief's primary responsibility is to monitor and oversee the department's response while not becoming too directly involved in any one function. Creating ties to any one part of the scene will reduce a chief's ability to perform duties as well as prevent the chief from remaining a leader in this type of situation.

Establishing an incident command system is of paramount importance. All departments must ensure that they have a system in place and that each person knows his or her role. Upon arrival, the incident command system should be set into motion immediately. Personnel should be assigned tasks, and channels should be set up for communication. In most cases, this entire system can be implemented before the chief arrives on the scene.

The chief must ensure that each member of the team is performing and troubleshoot any situations or problems that may arise between personnel, which is always an important factor to consider when dealing with situations involving mutual-aid and joint operations. The chief must watch over personnel and be prepared to force people to rest. Often those who are most determined to remain on scene, especially those in command positions, are those who need rest to remain in control and make good decisions. Staff rest and rotation are key, as are keeping calm and offering reassurance and a supportive presence.

WMD's Disruptive Potential

At Ground Zero

In the event of an actual WMD attack, law enforcement must know the dangers associated with responding to such an incident as well as the necessary protective actions to take to protect the public and themselves. They must pay careful attention to issues such as secondary devices and multiple attacks as well as the protective principles of time-distance-shielding. Awareness-level training is essential.

Assistance to victims is among the first priorities of emergency personnel responding to the scene of a WMD incident. However, all first-responder personnel should remember that in any NBC (nuclear, biological, or chemical) incident, supervisory personnel must be alerted to the situation as soon as possible to secure the necessary protective equipment for the first responders and mobilize resources. Responding personnel who enter the target area without proper protective gear may themselves become affected, thus rendering themselves unable to perform their duties and adding to the burden of remaining emergency personnel. Therefore, except in an extreme emergency, emergency personnel should not enter the affected areas unless they wear protective equipment, or until the appropriate authority determines that such equipment is unnecessary.

In some instances, assistance to victims may include not only evacuating the area or rendering medical care, but also neutralizing or mitigating the NBC material used in the attack. For example, ventilating the area may serve to dilute nerve gas or other chemical substances used in the attack. However, no such step should be taken rashly, as accelerated release of the agent into the atmosphere may endanger others, especially in the case of an incident involving biological agents. It may be necessary to leave this step to qualified personnel; in any case such action should not be taken prematurely.

Communities Miles Away

In the event an attack occurs elsewhere, law enforcement should be prepared to take affirmative action to ensure public safety in their geographical area of responsibility. A visible and professional police presence at vulnerable areas must be established. Strategic locations such as traffic control points, transportation centers, water supplies, communications facilities, plants, government buildings, financial institutions and other high-profile locations should be the object of police protection.

An incident command operation should be implemented with personnel, including civilian volunteers, placed on notice of possible call up, and available resources identified and updated. Chiefs should make public statements about the readiness of the community to handle an incident should one occur, and remind the public that calmness and respect of others are important at this time. When possible, chiefs should also ask the public to provide information of suspected activities.

Procedures should be developed to rapidly disseminate intelligence essential to the law enforcement mission. Law enforcement personnel should also be trained to gather intelligence in the course of their activities, whether in direct response to an attack or not. In each terrorist event, there will be a practice area and a staging area before the attack. Information about suspicious movement and activities should be developed locally. In the September 11 attacks, the terrorists had started moving around the United States, often staying in hotels in both large and small cities. In one suspicious incident, for example, two men who checked into a small-town hotel for a week never allowed the housekeeper to enter it. The housekeeper had to hand clean towels through a door that was barely cracked. These men are being investigated as part of the terrorist attacks.

Intelligence

Gathering intelligence does not stop once the attack is made. Important pieces of information can still be learned that leads to the mitigation of the damage, the prevention of other attacks, or the capture of the perpetrators.

Human Intelligence and Other Special Assets

Police departments have informants. Some are officially registered; others may be informal street contacts. In a real terrorism emergency, these informants—who are often plugged into the criminal and most notorious elements in a community—may be the first to detect something unusual in a town or city. What they pick up on the street may have a bearing on a terrorist incident or a looming threat. Regardless of their criminal expertise, in a time of crisis, informants should all be contacted and alerted that the police are looking for any and all information on terrorism and security threats.

Communications

From the beginning to the end of the event, the critical incident communication model should be in place. A communications officer should be assigned to oversee the physical and procedural aspects of voice and data communications. Following a process established during the preparation and training stage, the system should be activated and actively managed in support of the incident command. Physical security of the communications assets should be given a high priority. The most vulnerable points of a system will be in the physical control of access to hardware, facilities, and antennae sites. A buffer zone should be created to protect these sites and prevent unauthorized persons from having access and the opportunity to harm the communications system and its personnel.

Communications personnel should be prepared for a long-term operation. This

will require that personnel be used and rationed effectively. Requiring all personnel to report to work at the inception of an incident may result in no personnel being capable of working 12-18 hours later. Power supplies, especially batteries, will also have to be rationed and replaced in accordance with their capabilities. Battery life will be significantly shorter when portable radios, cellular phone, pagers, and mobile computers are being actively used. A communications supply officer should be prepared to replace batteries and immediately begin the refresh and recharging process to ensure that wireless devices can meet the demands of continuous operations. Backup power sources for dispatch centers should also be prepared for immediate and long-term operation at the beginning of a critical incident. The planning process should have revealed any problems with an alternate power source.

Pre-assigned procedures will ensure that information is exchanged as efficiently as possible, given the situation and the system being used. Field personnel should know what the primary and alternate communication procedures are in advance. In some cases, in the event of a total failure of mobile and wireless communications, officers may be tasked with responding to pre-assigned staging areas. The incident itself will create enough confusion for field personnel and command officials. Training and rehearsal will help reduce confusion relating to implementing policies and procedures. Most points of information exchange will be defined in advance. For example, the need for fire-to-police, police-to-EMS, and police-to-police communications should be clearly understood. The incident may present unique communication requirements not considered before the event. Incident commanders and other leaders should think not only about how to secure these unique assets, but also about how to communicate with them once they are secured. A dump truck, wrecker, cherry picker, or front-end loader will be of limited use if command officials are unable to efficiently communicate with the operator during the operation. If direct communications are not available, then communication through a dispatcher or a field unit assigned to the equipment is recommended.

As far as is practical, incident commanders should provide field personnel with global situation reports. During long-term operations, when personnel are kept apprised of the big picture, they are more likely to remain committed to the operation, are better able to endure longer hours in support of the operation, especially in mundane tasks, and are less inclined to gravitate to the center of the incident unless directed there.

Transportation

Emergency responses to incidents involve both rescue and enforcement activities. Emergency vehicles and personnel need immediate access to the scene, and the general public will expect to be able to evacuate. Designated highways can be identified as evacuation routes, and law enforcement must be available to direct motor vehicles away from an incident, using alternate routes and possibly changing the flow of traffic. Other modes of transportation, such as railways, buses, and ferry systems, should be identified as part of the rescue and evacuation process.

Secondary Response

The emergency phase continues with a secondary transportation response system, usually implemented within hours of the initial response. Heavy-duty equipment, such as cranes, bulldozers, and generators, may be required to assist in the rescue operations. Equipment of this size and nature is usually transported by commercial vehicles. Transportation managers have to work with federal and state regulators to determine if regulations normally applied will be waived, such as oversize and overweight permits, and hours-of-service regulations for operators. Other vehicles will be transporting food, medical supplies, and equipment to emergency rescue workers. Staging areas for these items must be established at an off-site location, which should be communicated to transportation logistics personnel. These staging areas alone will alleviate congestion, since only requested supplies will be transported on an as-needed basis to the affected area.

Traffic posts that are key to ingress and egress at the affected area must be designated during this phase. Law enforcement personnel must staff these posts in order to manage the flow of traffic into the affected area. Only authorized personnel with security clearance and their vehicles should be allowed access to the site. An indirect consideration of transportation management is the on-scene response by dignitaries and public officials. Successful long-term recovery depends upon the economic and governmental systems' ability to marshal resources in an efficient manner; thus, the inevitable political involvement needs to be accommodated.

Incident Management

The use of a WMD is an unusual occurrence that threatens the loss of life or injury to citizens and severe damage to property and requires extraordinary measures to protect lives, meet human needs, and achieve recovery. It is an extreme social crisis in which individuals and their social systems become disorganized and dysfunctional. The first few hours are chaos. However, this period may be actually referred to as the stabilization period—that time from when a critical incident begins to the point that adequate resources are on scene and under the control of a command structure, and human suffering and the unnecessary loss of life and/or property no longer occur.

A number of characteristics of this initial period are observable and important in order to understand what actions first responders should take:

- Local and area resources will move into the area, adding to the confusion and increasing the potential for blocking limited access into the stricken area—also known as resource convergence.
- Early responders will have difficulty assessing the true nature and scope of the incident.
- Responders, particularly early in the response, will only have limited resources for assignments for tasks that need to be performed.
- Critical decisions will need to be made: Who is in charge? Where is the command center located? How does command decide which primary objectives are to be assigned to the limited resources immediately available on scene?
- Certain determinations need to be made to protect the lives of the injured and those in the area of the incident, whether they are citizens or responders.

Common Problem Areas

All critical incidents have common problems that need to be resolved:

- *Direction and control:* How is a command structure established to provide authority under which the responders are controlled and their actions directed in a coherent manner while striving to achieve those objectives necessary to stabilize the incident?
- *Resource allocation and utilization:* In addressing this problem, can the command structure mobilize adequate resources with which operational and support functions can be implemented?

- *Communications:* How can communications carry on and resolve the limitations affecting effective communications?
- *Stress:* How can we reduce the effects of stress on our decision making and interpersonal reactions?

Medical Treatment

The highest priority of emergency response personnel during the initial response is to save lives, and it is in the first hour that significant saving of lives can occur. First-arriving personnel must know what actions to take to initiate the stabilization process.

The one-hour period begins at the point an injured person suffers serious trauma. It is during this 60-minute window that a person's chances of surviving are greatest. The longer it takes to get competent medical attention for the injured, the less chance the victim has of surviving. Therefore, the first responders must act together quickly to initiate and support life/safety activities. Only limited time is left to actually improve the survivability of the severely injured.

When a crisis occurs, human beings revert to doing what they've been trained to do, and in a way they respond routinely. This is why some personnel, supervisors and commanders included, may perform such tasks as helping to move the injured or deceased while important command tasks go unattended. In this emotional environment, personnel at the scene will be expected to make a variety of decisions and take actions to reduce the loss of life and decrease casualties as well as minimize property losses. Citizens and department personnel alike will expect commanders to take appropriate steps to direct the control of the incident.

Resource Management

Without adequate resources to fulfill missions or assignments, the commander of an operation may not be able to take appropriate steps to properly manage the situation.

There are two deployment options for taking control of the resources converging into the area of an incident: deploy them directly to assignments or route them through staging areas prior to assignments.

Direct deployment: Direct deployment is done either by personal instruction at a location away from a staging area or via the dispatcher. In most cases, direct deployment applies resources immediately to an incident's perimeter, securing the scene and routing traffic. The advantage of this method is that the assignments can be given out faster. This method appears to help police quickly take control of the perimeter, but it has some serious disadvantages at the scene, including the following:

- Information concerning the threat to personnel may be non-existent, limited, or even flawed.
- The person assigning them may lose track of who is where.
- Personnel taking positions may not have proper equipment.
- This procedure consumes valuable airtime.
- Traffic congestion due to resource convergence may restrict other operations.

Deployment via staging: The staging area is that location where incident personnel and equipment are assigned/collected on an immediately available status. Personnel and equipment will be held at the staging area until called for or until their portion of a mission requires departure. Deployment via staging occurs when all personnel, unless otherwise directed, are instructed to report to the staging area, where they are briefed and their equipment needs addressed. They are then sent on to their assignments.

The advantages of deployment via staging include better-informed, more effective personnel who face a reduced threat, because they understand the nature, location, and description of the threat. Less airtime is needed because the process of briefing the personnel occurs face-to-face. This method has one major disadvantage: it takes more time.

Operational Objectives and Unity of Command

One of the central marks of well-commanded critical incidents is that people knew what had to be done and in what order and how their portion of the operation linked with others. The ability to assess an incident and successfully identify the central objectives is a necessary skill for commanding an incident. In too many instances, command personnel are confused and unable to determine central objectives and act on them. Early in an incident, when resources are limited and/or disorganized, objectives must be clearly identified, prioritized, and acted upon.

In most bombing incidents, personnel from other agencies will help. A fundamental principle is that no one should work for more than one supervisor. Under the concept of unity of command, all personnel assigned to achieve a shared objective should be under the supervision of only one person.

Determining a Command Structure

Simply stated, a command structure's sole purpose is to link individuals and agencies together to achieve the objectives of an incident and to do so in a coherent manner that uses available resources with a maximum of economy.

This is likewise the purpose of the incident command system (ICS), required by federal law to respond to hazardous materials incidents. By definition, alleged or real explosive devices contain hazardous substances; therefore, ICS should be employed.

While this document does not provide the opportunity to discuss at length what ICS is and how to use it, any commander or supervisor who is likely to respond to such incidents should be fully competent in the use of ICS, particularly during the initial response to these incidents.

The ICS organizational structure develops in a modular fashion based upon the type and magnitude of an incident.

Community Outreach and Information

As soon as an agency learns about an incident, communication with the media should begin through the pre-defined process. Designated agency spokespersons should be immediately briefed and deployed to provide the media with any critical information necessary to ensure public safety.

As an incident unfolds, there will be mass amounts of information being rapidly received. Not all of this information will be accurate. While most critical information should be confirmed, some information may be released that is not accurate and will later require clarification or correction. The agency spokesperson should clearly state when information being released is confirmed or is speculative. The media should understand the confusion that ensues in a critical incident and the misinformation that may result in the flows of multiple communication channels.

The News Media

Law enforcement personnel naturally see their mission as uppermost in priority. Since the crisis has a high visibility, law enforcement personnel are acutely aware that their performance must be procedurally correct. On the other hand, the news media expect that their report-

Six-Step Incident Response Process

Step 1: Size Up the Situation

Answer the following questions:

- What is the nature of the incident?
- What hazards are present?
- How large an area is affected?
- How can the area be isolated?
- What location would make for a good staging area?
- What entrance/exit /safe routes would be good for the flow of response personnel and equipment?

Include the following information in size-up reports:

- The unit designation
- A description of the situation
- Obvious conditions (e.g. hazards)
- Initial actions taken
- Obvious safety concerns
- Assumption, identification and location of command post
- Request or release of resources

Step 2: Identify Contingencies

To the extent possible, anticipate points in the incident management process that may fail and determine alternative steps in advance that can be implemented if necessary. Murphy's Law and its corollaries apply and bear repeating:

- If anything can go wrong, it will.
- Nothing is as easy as it looks.
- Everything takes longer than you think it will.

Step 3: Determine Objectives

Meaningful objectives are:

- Measurable
- Used to monitor incident progress and establish priorities
- Based on size-up reports and identified contingencies

Step 4: Identify Needed Resources.

Determine the following:

- What resources are necessary?
- Are they on hand?
- Where might we get them?
- How long will it take?
- What is available from other agencies?
- Are there any special requirements?

Step 5: Build an Incident Action Plan and Management Structure

Identify the following:

- Responsibilities
- Chain of command
- Coordination

Step 6: Take Action

Incident stabilization involves the following steps:

- Establishing command
- Mobilizing resources
- Setting up a staging area
- Isolating the area
- Treating and assisting the injured
- Setting up entrance, exit, and safe routes
- Issuing warnings
- Initiating evacuation
- Establishing liaison

From IACP Project Response: Preparing Law Enforcement for Y2K, International Association of Chiefs of Police, Alexandria, Virginia, 1999.

ing function will be facilitated by law enforcement. They want to see and hear things that are denied to curious bystanders, and they expect cooperation from law enforcement personnel.

The best plan is to establish a briefing area for the news media. The media should have an observation perimeter that can provide essential close access. The area should be marked with distinctive colored tape and established within the first 30 minutes of a crisis. An officer should be detailed to check credentials, control access to and movement within the secured perimeter, and secure the safety of the media equipment.

Different media require different settings. Television needs video and film. The crews will be concerned about lighting and shadows as well as voice quality, and will need room for trucks and transmission dishes. Radio will require a quiet place to hook into telephone lines. The press will want to probe deeply into certain aspects of the story and may require some extra attention and additional interview opportunities.

The Public Information Officer

A single spokesperson should be designated the public information officer (PIO) to brief the news media. The PIO should meet with media personnel and brief them in detail on the incident. The PIO must project a strong, take-charge image to the media and give the distinct impression that the department will provide all information throughout the crisis. The PIO needs to screen out conjecture and rumors, and should avoid making the media scratch for their own stories and facts, since this will result in mistakes even beyond the misinformation natural to a crisis event.

The PIO may need to request time on radio and television stations to share information with the public about the crisis, especially what role the public should play in coping with the situation, and other health and safety issues.

The PIO should define the crisis situation accurately and objectively for the media as soon as possible. Initial statements should be made early, perhaps 30 to 45 minutes after enforcement arrives and after the media perimeter is secure. The PIO should provide basic information regarding on-scene services. High-ranking officials (governor, mayor, council members) should be present, briefed, and prepared to comment. Comments from these elected officials will help place the crisis in an appropriate perspective.

During the attack or incident, the media should be allowed access to the incident for reporting purposes to the extent that they do not hamper rescue efforts or compromise law enforcement operations. Some members of the media waive certain safety precautions in order to document incidents; however, their access may be limited in situations that present extreme danger to all but the most protected and trained law enforcement personnel.

At some point, the agency head should make a statement, since as head of the agency, he or she carries great credibility and presents a compelling presence. The public will look to the agency head, not a spokesperson, for the ultimate feeling of security. The agency head's statement should be candid about the unfolding events, but at the same time should be reassuring, emphasizing prior training and preparation, and outlining the agency response.

If the attack or incident does not occur in or near the jurisdiction of the agency, agency spokespersons should still maintain contact with the local media. Regular briefings of the news media need to be established in time for the reporters to meet their deadlines. Information regarding the escalation of law enforcement presence and awareness should be emphasized. Messages should be disseminated to ensure that the agency is making efforts to maintain the integrity and safety of the community.

III. AFTER AN INCIDENT: FOLLOWING THROUGH

Helping the Healing

Even after the on-scene situation has been dealt with and is relatively complete, the chief's duties are still far from over. Many departmental matters follow a situation such as this. Employees have worked long and hard for the department and must be compensated. Overtime hours must be calculated, financial and personnel assistance (if needed) must be requested and pursued, and the needs of employees must be addressed.

In addition, emotional needs of staff are often hidden or ignored but need to be addressed. Critical incident stress debriefing personnel must be made available for officers who require such services.

Chiefs should be available to the media and the community to help citizens strike a balance between prudent reaction and paranoia as they react to the event. Chiefs must act to promote appropriate fear reduction, cautioning citizens to remain alert. In most communities, the chief's presence and the tone set are critical factors in community healing.

Chiefs will have to reduce after-incident workloads for staff, and begin the final disposition activities the incident requires, particularly that of writing a final incident report summary. Bringing in support staff or even consultant staff to work with officers to create that document and assist in other post-incident matters can be very helpful. A post-incident evaluation should be performed to evaluate response and discuss what went well and what can be changed in the future.

Recognizing outstanding and/or heroic actions by those at the scene is an important act for the entire community. Chiefs can take the lead here, helping to identify those individuals worthy of recognition, designing the ceremony and awards to be given, and making such events open to the media and the entire community.

Crime Scene

The investigative role of local police following a WMD attack may be limited. Investigation and attempts to apprehend the perpetrators will usually be in the hands of federal agencies, with local law enforcement officers working on the investigation in a secondary role. Local officers should, however, cooperate in the investigation in any way possible. Turf issues have no place in investigating a WMD incident.

In the case of an incident involving detonation of a nuclear bomb, the blast will destroy virtually all physical evidence as well as most of the possible witnesses to the planting of the device. However, some scientific investigation techniques may help trace the source of the weapon, and the perpetrators may still be identified through tips and information derived through national or international intelligence sources.

Radiation dispersal attacks and attacks employing chemical or biological weapons will normally leave physical evidence that can be used to identify the perpetrators. In addition, unlike the nuclear explosion, with the other types of WMD attack, a number of eyewitnesses may survive the attack and, though injured or ill, may still be able to give information to the authorities about the incident.

In any type of WMD attack, apprehending the perpetrators will be complicated by the fact that in many instances they will have left the jurisdiction—perhaps even the country—before the detonation. Although domestic terrorists will often remain within the United States, it may require national and international law enforcement, intelligence, and diplomatic efforts to track down and arrest perpetrators who have fled to another country. As illustrated by the terrorist attack on Pan Am 103, if the perpetrators have succeeded in reaching certain safe havens abroad, prosecution may be impossible even if the culprits are identified. The Pam Am bombing occurred December 1988 over Lockerbie, Scotland, killing 270 people. Not until 11 years later (April 5, 1999) did the Libyan government turn over two former intelligence operatives identified as the perpetrators.

Local, state, and federal law may affect a police department's ability to gather information on individuals, even during a terrorism crisis. For instance, data systems that collect information about individuals and are funded by federal grants must conform to federal guidelines for intelligence gathering. Similar laws may govern grants from other sources. In addition, many municipalities and police departments have local laws or guidelines on when and under what circumstance police can collect and/or computerize non-criminal information about individuals. Knowing the laws that govern a particular jurisdiction and seeking legal counsel when in doubt are important factors in conducting the investigation.

Psychological Issues

The department must support its personnel and encourage them to support each other. Following a disaster or serious act of violence, police and other emergency responders may suffer from stress-related ailments such as insomnia, depression, anger, headaches, and ulcers.

Debriefings by experienced counselors 24-72 hours after their involvement with a traumatic incident may reduce the stress experienced by affected individuals. Debriefing serves as an opportunity for individuals to express their thoughts and feelings about what happened, and how it was handled. It also gives the debriefing team a chance to alert employees to the symptoms of posttraumatic stress disorder (PTSD) and to identify individuals who might need further counseling. Disseminating information and holding debriefings will help officers understand that their stress feelings are normal and that the symptoms will subside in time. Police departments can utilize police psychologists, police chaplains, and local victim service personnel/counselors to assist. Employee assistance programs for follow-up support can include individual counseling, peer counseling, family counseling, and proactive stress training.

Leaders should ensure that they take care of themselves as well. In a very real sense, they are setting the standard for getting necessary help and acting as role models in critical incident stress management.

A post-incident evaluation should be held by victim-centered crisis response team to evaluate response and discuss what went well and what can be changed in the future. This may include a debriefing with the victim-centered crisis response team, the victims and the surviving family, as appropriate, to get feedback regarding effectiveness of the care-

giver response

In conjunction with the victim-centered crisis response team, police should hold debriefings with community members and leaders to discuss fears and concerns, and to continue a message of calmness to avert anxiety and possible community tension. Another good step is to allow community opportunities to grieve victims and express gratitude to rescue workers by setting up memorials, vigils and/or foundations.

Rumor Control

A crucial role for any chief in the aftermath of a terrorist incident is controlling the rumors and fear within a community. This is best done through quick, reassuring community outreach and through the establishment of a rumor-control number (which can also be marketed as a community-tips hotline). As important as the tips that come in is the role that skilled police operators can play in reassuring the callers. Terrorist incidents are designed to strike fear into citizens, and that fear can increase exponentially if rumors are not contradicted quickly. Through various forms of media, police can educate the community about the symptoms of potential exposure to biological and chemical agents (if applicable), and provide information about who to contact, and when and where to receive medical attention. Key civic leaders who can help control rumors in a crisis (and pass on valuable and credible tips from worried citizens) include the obvious elected leaders and civic association heads. An often-overlooked resource are religious leaders, who provide a moral center and serve as sounding boards, commanding great respect from any community in a crisis.

Racial/Ethnic Backlash

As the events of an attack unfold and suspects are identified, the chief must be prepared to respond. A major focus of the chief's response will be preventing backlash against any segments of the community that some consider responsible. The crisis of terrorism can stir a wide range of emotions in people directly affected by the events as well as those indirectly affected. Leaders should encourage people to channel their feelings of fear, anxiety, sadness, and anger into positive, community-centered actions.

Opportunities to come together can help focus energies productively while calming and comforting people. A strong statement by law enforcement leaders that such acts of hate will be investigated and prosecuted to the fullest extent of the law can also provide some needed reassurance while deterring further violence.

Police must understand that the acts of hate crime and violence are experienced by the entire targeted community; its members' daily lives are disrupted by feelings of fear and vulnerability. The chief's response will be guided by what race or ethnic background the suspects appear to. Should the victims of hate crime or violence come from a certain ethnic or religious group, the chief may need to increase police presence to provide the assurance of safety near that group's homes, businesses, and houses of worship. Their fears about being targets for violence are real, and they need to know that police are sensitive to their concerns.

Assuming all the things recommended in the pre-incident section were put in place, the chief will be able to contact the leaders of that segment of the community who are potential targets for retribution. Keeping those lines of communication open and moving both ways during this time is absolutely essential and will reassure everyone that the police are there to protect them and could even generate information that might be of interest to those investigating the terrorist attacks.

Unfortunately, some individuals will decide to lash out at others because of their feelings of hatred and anger. In managing the crisis, law enforcement must watch for signs of unrest and prepare to prevent acts of retaliation and hate. Some citizens may direct their actions at parties they perceive to be responsible for or connected to the crisis. They may engage in threats or harassment or direct acts of violence such as vandalism or assault as a way to retaliate. Law enforcement needs to be aware that a crisis in the community or country will inevitably result in some illegal activity directed against people, groups, or organizations believed to be associated with the act(s) of terror. In addition, law enforcement should seek out opportunities to communicate with and calm vulnerable members of society. Law enforcement should reiterate the department's policies on intolerance and harassment as well as laws relating to hate crimes. Officers should continue to promote messages of tolerance towards others within community.

All of these responses require extensive training on hate crimes and their impact. Beyond basic investigative strategies, officers need to understand the continuum of hate violence (from incidents to crimes) and how it affects the victim. An officer's ability to effectively interview a traumatized victim may depend on his or her training on the emotional, psychological, and practical impact of hate crime.

Victim Assistance

A number of lessons were learned from previous acts of terrorism including the Oklahoma City bombing and the bombing of Pan Am Flight 103. While performing the necessary tasks required by the job, police need to be sensitive and understand the unique needs of the victims and their families. Some basic steps should be implemented to address the needs of those people. The following recommendations were offered in an Office for Victims of Crime report on responding to terrorism victims (NCJ 183949):

- Whenever possible, responding agencies should avoid unnecessary delays in death notification and the release of victim remains to families and to handle notification in a sensitive manner. In the immediate aftermath of a domestic terrorism disaster, local officials should consider establishing a centralized compassion center where victims can go for information, crisis counseling, and privacy.
- Mental health services should be made available in the immediate aftermath of a terrorist act, and plans should be made for assessment and long-term provision of services for victims and responders.
- Local, state, and federal agencies responding to victims of a terrorist act should consider establishing an "unmet needs" committee or task force that includes private organizations to ensure that the needs of victims are identified and addressed and that all of the unavailable resources are coordinated and used on behalf of the victims.
- Agencies serving victims should work together to develop protocols for recruiting, screening, training, and supporting volunteers who work with terrorism victims and their families.

Agents should disseminate information, utilizing the media, on normal reactions to critical incidents, suggested coping skills, including obtaining mental health assistance, and the effects of chemical or biological agents. Agents should explain symptoms, and provide information about who to contact and when and where to receive medical attention.

Bibliography and Resources

Web Sites

- http://www.fbi.gov/
  (FBI)
- http://www.ojp.usdoj.gov/ovc/
  (Office for Victims of Crime)
- http://www.atf.treas.gov/
  (ATF)
- http://www.fema.gov/
  (Federal Emergency Management Agency)
- http://www.ndpo.gov/
  (National Domestic Preparedness Office)
- http://www.state.gov/
  (Department of State)
- http://www.usdoj.gov/dea/programs/epic.htm
  (El Paso Intelligence Center)
- http://www.llnl.gov/str/Imbro.html
  (Weapons of Mass Destruction website)
- http://www.firstgov.gov/featured/usresponse.html
  (U.S. government information and resources)
- http://osldps.ncjrs.org/
  (Domestic preparedness support information clearinghouse)
- http://www.redcross.org/
  (Red Cross)
- http://www.iir.com/riss/default.htm
  (Regional Information Sharing Systems)
- http://www.nipc.gov/
  National Infrastructure Protection Center

IACP Publications

- *Training Key #484*, "Weapons of Mass Destruction, Part 1," International Association of Chiefs of Police, Alexandria, Virginia, 1998.
- *Training Key #485*, "Weapons of Mass Destruction, Part 2," International Association of Chiefs of Police, Alexandria, Virginia, 1998.
- *Training Key #486*, "Weapons of Mass Destruction, Part 3," International Association of Chiefs of Police, Alexandria, Virginia, 1998.
- *IACP Model Policy*, "Criminal Intelligence," International Association of Chiefs of Police, Alexandria, Virginia, 1998.
- *IACP Model Policy*, "Police-Media Relations," International Association of Chiefs of Police, Alexandria, Virginia, 1992.
- *IACP Model Policy*, "Memorandum of Understanding," International Association of Chiefs of Police, Alexandria, Virginia, 2001.
- *Responding to Hate Crimes: A Police Officer's Guide to Investigation and Prevention*, International Association of Chiefs of Police, Alexandria, Virginia, 1999.

Other Publications

- *Local Officials Guide to Domestic Terrorism: Resources for Local Governments*, National League of Cities, 2001, www.nlc.org
- *Responding to Terrorism Victims: Oklahoma City and Beyond*, Office for Victims of Crime, U.S. Department of Justice, 2000.
- *Project Response: Preparing Law Enforcement for Y2K*, International Association of Chiefs of Police, Alexandria, Virginia, 1999.

Other Organizations

- Concerns of Police Survivors (COPS)
  (573) 346-4911
- Public Safety Officers' Benefits Program
  (888) 744-6513

The International Association of Chiefs of Police (IACP) stands ready to support and assist all law enforcement agencies in addressing problems and issues arising around the world. Through our network of communications, information, and distribution, we recognize our responsibility to serve our members who face difficult times now and in the future. The strength we enjoy is the result of committed members working together for the good of all law enforcement throughout the world.

For more information on the various services and products IACP provides its members, visit our website (www.theiacp.org), contact us at information@theiacp.org, or write to

The International Association of Chiefs of Police
515 North Washington Street
Alexandria VA 22314