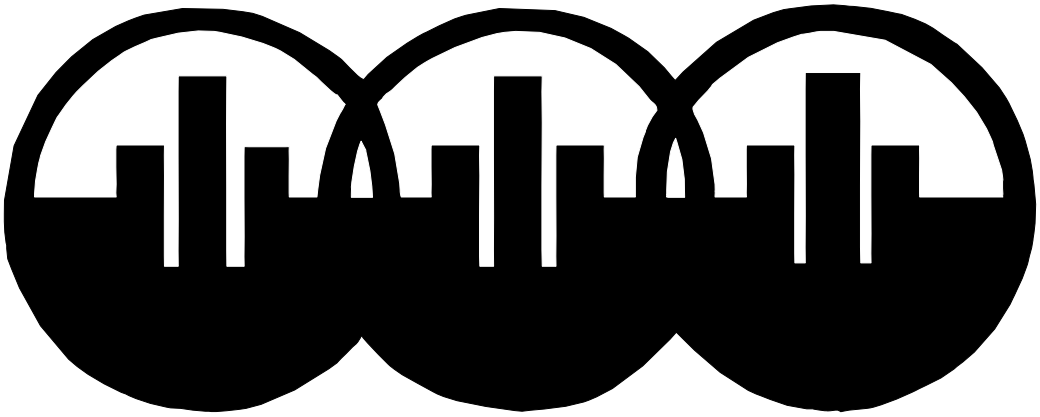
NATIONAL LEAGUE OF CITIES



HOMELAND SECURITY:
PRACTICAL TOOLS FOR LOCAL GOVERNMENTS

November 2002
(revised)

TABLE OF CONTENTS

A Message from the Working Group on Homeland Security

The terrorist attacks on September 11, 2001, had far-reaching impacts on American life. Among the many things that changed were the roles and responsibilities of municipal governments across the country. Over the past year, local officials have been called upon to play a new and expanded leadership role in ensuring the security of their hometowns and in restoring the confidence of a shaken public.

In January 2002, NLC President Karen Anderson, Mayor of Minnetonka, Minnesota, established a special Working Group on Homeland Security. The group's charge: to serve as a front-line resource on the issue for the National League of Cities and to advise the NLC leadership and staff on emerging topics and local needs.

It is clear from the group's work over the past year that homeland security is now a top priority for cities and towns of all sizes and in all parts of the country. It will continue to be a priority.

Homeland security is . . .

- A responsibility that America's cities and towns are ready, willing, and able to assume as the front line of hometown defense;
- A responsibility that will not go away; and
- A responsibility that will require dedication of new public funds to ensure long-term readiness for threats that were only considered a remote possibility before September 11, 2001.

At our first meeting, the members of the working group reached three conclusions about homeland security that have guided our activities (see box). In the months since, we have affirmed that the primary goal of every city in America – large or small, urban or rural, inland or on the coast – is to be a safe city. That means a place where residents feel safe, secure, and confident that local leaders know what to do in case of an emergency.

This guidebook is designed to help local leaders achieve the goal of making their cities safe. It is being published in tandem with a companion document that focuses on federal resources for local governments working on these issues (see page 29).

The primary goal of every city in America is to be a safe city, a place where residents feel safe, secure, and confident that local leaders know what to do in case of an emergency.

Recognizing that the precise steps local officials take to ensure hometown security will be as individual as the communities they govern, this document provides some basic tools for navigating this complex issue. It provides a framework for action, issues to think about, examples of local approaches, and contacts for specific information. These resources will be updated and expanded on a regular basis to include new issues, new examples, and new approaches as they come to light.

As local officials who share in the enormous responsibility of securing our hometowns, we have appreciated the opportunity to work together to provide support, guidance, and resources to our colleagues and friends across the country.

We applaud your interest in doing a better job securing *your* hometown, and we wish you all the best.

2002 NLC Working Group on Homeland Security

Co Chairs
Michael Guido, Mayor, Dearborn, MI
Mary Poss, Mayor Pro Tem, Dallas, TX

Members
Rocky Anderson, Mayor, Salt Lake City, UT
Patrick Avalos, Councilmember, Pueblo, CO
Michael Bahun, Councilmember, Kettering, OH
Brenda Barger, Mayor, Watertown, SD
Patricia Dando, Councilmember, San Jose, CA
C. Virginia Fields, Manhattan Borough President, New York, New York
Dan Furtado, Vice Mayor, Campbell, CA
Ed Garza, Mayor, San Antonio, TX
Karen Geraghty, Mayor, Portland, ME
Neil Giuliano, Mayor, Tempe, AZ
Glenda Hood, Mayor, Orlando, FL
Charles Jennings, Commissioner, Arkansas City, KS
Michael Keck, City Director, Little Rock, AR
Sylvia Lovely, Executive Director, Kentucky League of Cities
Paul McLaughlin, Councilmember, International Falls, MN
Brian O'Neill, Councilman, Philadelphia, PA
Evelyn Turner Pugh, Councilor, Columbus, Georgia
Anthony Williams, Mayor, Washington, DC

Ex Officio
Karen Anderson, Mayor, Minnetonka, MN; NLC President

Introduction

As the events of September 11, 2001, made only too clear, terrorists attack cities. Cities and towns are population centers, as well as hubs of transportation, communications, and economic activities. Cities and towns also provide the largest variety of targets—tall or significant buildings, federal installations, centralized infrastructure—that appeal to terrorists because of the potential to impact large numbers of people.

The fact that cities are the most likely targets of terror means city leaders throughout the country play a critical role in preventing and responding to attacks. Without a doubt, the most important responsibility of municipal officials is to coordinate disaster response efforts during the first 24 to 72 hours after any emergency, a critical time period during which state and/or federal authorities may not be sufficiently equipped to help.

The topic of disaster preparedness and response confronts local elected officials with a wide range of tough questions, including:

- What is the likelihood of an attack in my community?
- What will it take to protect my community?
- How can homeland security be incorporated into my community's current emergency plan?
- How can I make homeland security planning a priority while meeting the day-to-day needs of my community?

Without a doubt, the most important responsibility of municipal officials is to coordinate disaster response efforts during the first 24 to 72 hours after any emergency.

Within this document, NLC has compiled the most up-to-date information available to help you find specific answers to these and other questions.

No single government agency at the local, state, or federal level possesses the authority or expertise to act alone on the many complex issues connected to terrorism. Coordinating planning and assigning responsibilities across and among the different levels of government is an evolving process. As a result, NLC will continue to update this document as things change. Our goal is to provide you with the best and the latest information so you can keep your homeland security planning efforts fresh and up to date.

PART ONE: WHAT YOU CAN DO

The NLC Working Group on Homeland Security concluded that local elected officials have five primary roles to play in ensuring the security of their hometowns. Here's what you can do:

1. **Plan**
2. **Practice**
3. **Communicate**
4. **Prepare Your Local Government**
5. **Aggressively Seek Funding—Find and Use Resources**

The remainder of this document provides more information on how local officials can fulfill these roles, as well as examples showing how cities and towns across the country are doing exactly that.

IMPORTANT: The Working Group is fully aware that these are not the only roles that local elected leaders play on this issue. You may identify other ways you can help make sure that your community is doing everything it can to prepare for and prevent attacks. The key is to work with others to figure out the best approach for your hometown—and then to get to work making it a safer place.

1. Plan

> "Rather than create different emergency response plans for every type of natural or manmade disaster, communities should develop one overriding plan applicable to most situations. Leaders of cities and counties must agree upon, achieve, and maintain a minimum level of preparedness with possible current resources, then build upon those capabilities."
>
> ·· *Preparing for Terrorism: What Every Manager Needs to Know* by Howard Levitin, MD, FACEP, International City/County Management Association (ICMA), 2001

As Dr. Levitin suggests, the best place to start your city's planning efforts for hometown security is with your current emergency plan. Every community has an emergency plan of some kind—whether it is for tornado or flood response, Y2K plans, reaction to a hazmat emergency, or law enforcement coordination for a public protest. The first thing you can do is to review and assess the plan (or plans) you have in place, together with your existing city/county disaster plans and mutual-aid agreements, and consider their applicability in the event of a terrorist attack.

Lessons from the Working Group on Homeland Security

- Define and communicate clearly who's in charge and who is responsible for specific response components.
- Be prepared to operate alone in an emergency for 24 to 48 hours before other local/state/federal support arrives.
- Plan for continuity of government during and after an emergency.
- Prepare boilerplate emergency proclamations, citizen alerts, and other important documents in advance so they can be put into effect immediately, and be sure to have all mutual aid agreements signed and in place.
- Make sure you are taking full advantage of technologies that can support and streamline emergency preparedness, response, and recovery.

As you review the existing plans, consider not just the obvious items (coordinating police, fire, and emergency management services), but other issues as well. For example, what you would need to do differently in the event of a biological incident? Or, how could you best coordinate transportation options to conduct an evacuation of your city or town?

Your Role in Local Planning. Local elected officials can find themselves playing a variety of roles in local emergency planning activities. Three important roles you can play are as coordinator, liaison, and representative.

Coordinator. As a local elected official, it is your job to coordinate critical city services such as law enforcement, emergency medical services, and social services. As you prepare and test your city's emergency plan, make a point of clarifying and defining the roles of each city department and each department head to prevent gaps or overlaps of function. This is why every city's plan should establish responsibility and points of decision-making authority. One of your most important responsibilities during an emergency event will be to meet regularly with department heads so you can continuously monitor the work of their departments and adjust functions and responsibilities as necessary.

Liaison. Local officials also will find themselves in the role of liaison among various federal and state agencies, city departments, the business community, and the public. In order to perform this role effectively, it is important to maintain regular contact with state and federal entities, such as the state police and the regional FBI office. Your job is to understand their roles as well as their needs in an emergency situation, and to communicate these roles and needs to city departments. Similarly, local elected officials should act as a link to city government for both the business community and the public, working to ensure that their needs and concerns are met.

Representative. Local officials also should act as representatives of their cities in the wider regional emergency planning effort. Most regions and metropolitan areas, regardless of size, have some kind of regional coordination effort in place, such as mutual aid agreements or transportation plans. Take advantage of these regional efforts and use them as a foundation for discussing regional emergency planning. If no regional entity exists, work to convene one. As a representative of your city, articulate your needs as well as the contributions that your city can make to a region-wide emergency plan, and work to build consensus among all jurisdictions about what needs to be done and how.

Assessing Local Risk (and Resources). Risk assessment is a critical step in community planning. Among the key questions: What could potentially be a target? In the course of this assessment, you will also want to work with your regional partners to identify potential targets in the surrounding communities.

Potential terrorism targets in America's cities include:

- Ports of entry – airports, harbors
- Water systems
- Energy supplies
- Transportation infrastructure – highways, roads, bridges, rail lines, tunnels
- Military installations
- Other federal facilities (buildings, research labs, nuclear plants)
- Schools/universities
- International borders
- Government buildings (city, state, federal)
- Stadiums, arenas, convention centers
- Other large buildings (high-rises), landmarks, monuments
- Communications and technology infrastructure

- Power plants
- Hospitals/medical facilities

Your city's plan also should include an assessment of your existing financial, personnel, and equipment resources. While the reallocation of some of these resources may meet most of your requirements, it is important to prioritize expenses based on the most serious risk factors in your community.

Issues to Consider. In addition to assessing your risk and the resources at your disposal, your hometown security planning should include serious consideration of such issues as the following:

- What other government entities and private organizations should be part of your planning?
- What is the nature or status of your relationships with these entities, and how can you build stronger ties?
- In the event of an emergency, what would the chain of command look like, and who should be notified first?
- Can everyone communicate—i.e., do they have the right equipment and are there any language barriers?
- How will you communicate critical information to citizens and those outside the immediate area?

Other Resources. There are a number of good resources on emergency planning for cities and towns. Two important sources of information and assistance for local officials are the Federal Emergency Management Agency (FEMA) and state municipal leagues.

Emergency Planning Should Include:

- City Administration
- Law Enforcement
- Fire/EMS
- Public Works
- Utilities (water, electric, gas, phone)
- Transportation
- Telecommunication
- Local FBI office
- State homeland security office
- State Attorney General's office
- County public health officials
- Local hospitals
- Neighboring communities
- Local businesses
- American Red Cross
- Community groups
- Council of Governments
- Local nonprofit organizations

FEMA. According to the Federal Emergency Management Agency (FEMA), a jurisdiction's emergency operations plan is a document that:

- Assigns responsibility to organizations and individuals for carrying out specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency, e.g., the fire department.
- Sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated.
- Describes how people and property will be protected in emergencies and disasters.
- Identifies personnel, equipment, facilities, supplies, and other resources available—within the jurisdiction or by agreement with other jurisdictions—for use during response and recovery operations.
- Identifies steps to address mitigation concerns during response and recovery activities.

For more detailed guidance from FEMA, visit the sites listed under Resources below.

State Municipal Leagues. The Kentucky League of Cities and the NewCities Foundation have developed a useful hometown security guide for public officials, in addition to holding a seminar on the topic in January 2002. The guide, which can be found on the Kentucky League of Cities website (http://www.klc.org/terrorism2.htm), identifies four steps in the hometown security planning process:

1. **Establish a Planning Team**. The planning team should be a broadly representative group, including law enforcement, fire/EMS, city administration, utilities, telecommunications, transportation, community representatives, and businesses.
2. **Analyze Capabilities and Hazards**. Gather information about current capabilities, plans, and resources (internal and external), and conduct a vulnerability assessment.
3. **Develop the Plan**. The plan should describe the city's emergency management policy; identify the authority and responsibilities of key personnel; outline the types of emergencies that could occur; and explain specific response procedures.
4. **Implement the Plan**. To ensure that the plan is implemented successfully, municipal officials and others should act on recommendations made during the vulnerability analysis; integrate the plan into day-to-day operations; coordinate it with other local, county, state, and federal plans; provide training; and evaluate and update the plan on a regular basis.

Other state leagues have provided similar information for elected officials in their states. Check with your league to see what's available.

First Steps for Preparedness

- Systematically evaluate current capabilities and deficiencies.
- Perform a risk assessment and vulnerability analysis of the community.
- Ensure that local hospitals are prepared to treat victims of a terrorist attack.
- Evaluate the current capabilities of the fire department's response to HAZMAT incidents.
- Meet with those responsible for emergency medical services to assess their current scope of practice as it pertains to terrorist events.
- Cross-train the appropriate responders in order to avoid having to create and fund additional response teams.
- Provide frequent, brief training programs to medical personnel to ensure their participation in the preparedness process.
- Develop mutual aid agreements with surrounding communities to ensure better use of existing resources during any type of disaster.
- Incorporate the business community into the planning process.

Source: Preparing for Terrorism: What Every Manager Needs to Know by Howard Levitin, MD, FACEP, International City/County Management Association (ICMA), 2001.

Examples

San Jose, CA (Population: 894,943). San Jose has a comprehensive and far-reaching civil defense plan to respond to terrorist attacks and other large-scale emergency incidents. Coordinated by the city's Office of Emergency Services, and developed with the full participation of the mayor, council, and department heads, the plan includes separate protocols for handling both non-terrorist disasters, such as industrial accidents, and terrorist incidents that frequently require more forensic investigation. While much of the plan is kept secret, it is known to involve the stockpiling of antibiotics to fight disease outbreaks and the use of gas detectors and robots to handle hazardous chemical releases. Also under the plan, doctors at area hospitals keep bioterrorism manuals on hand to help them quickly identify symptoms that point to a hazardous substance attack. The plan, which is funded by both the city and the federal government, includes the support of the San Jose Metropolitan Medical Task Force, a terrorism response unit that includes police, fire, and medical personnel.

Worcester, MA (Population: 172,648). Worcester has a security task force to prepare for and respond to acts of bioterrorism. In the wake of anthrax scares in the fall of 2001, the task force reviewed city policies, procedures, and preparedness for such things as disease testing, security and storage of potentially hazardous materials, and response to hazardous materials releases. Worcester officials also made recommendations concerning education, training, and deployment of emergency personnel, the procurement of special supplies and equipment, and the need for operational changes in city departments. Chaired by a city public health officer, the task force includes representatives from the police, fire, public works, emergency management, and city schools departments.

Pacific Grove, CA (Population: 15,522). Recognizing that it takes time for federal help to reach the scene of a large-scale terrorist attack, the Pacific Grove Fire Department and the nearby Naval Postgraduate Institute formed a partnership to develop a first-response plan. The partnership developed several response models, each based on a different terrorist scenario, and held simulation exercises for each one. All of the response models incorporate help and equipment from nearby cities.

Waterford, CT (Population: 19,152)**.** Following the terrorist attacks of September 2001, Waterford relocated parking for its fleet of 21 school buses. To allow for rapid evacuation of school students in the event of an emergency, the school buses are parked near the town's three schools and the volunteer fire department. In addition, public works employees are trained as back-up drivers in case regular drivers can't be located quickly.

Pittsburgh, PA (Population: 334,563). Two months after the September 2001 terrorist attacks, Pittsburgh formed a coalition of seven citizen groups to put together an emergency response plan. Six major issues are addressed in the plan: building safety; communication; health care; neighborhoods; schools; and transportation and utilities. The plan prescribes creating "communications redundancies" by using e-mail, faxes, and the Web to pass along vital information. It also calls for coordinating communication between the city and area health care providers. Under the plan, buildings taller than six stories must conduct evacuation drills twice a year, and mass casualty drills also must be conducted routinely. Last, but not least, Pittsburgh requires educational institutions to review their own disaster preparedness plans annually.

Saco, ME (Population: 15,822). In case of a natural disaster, or even a man-made technological disaster such as computer hacking, Saco has a strategy to safeguard its data and systems and ensure that city services continue to run smoothly. To test the strategy, the city held a disaster recovery workshop and simulation exercise focused on its information technology infrastructure. Representatives from all city agencies, as well as some from local businesses, participated in the simulation. Among the systems tested: back-up computer storage; telecommunications; and back-up power generation.

Tullahoma, TN (Population: 17,994). Tullahoma's Emergency Preparedness Committee develops strategies for dealing with a variety of emergency-related issues and enhances disaster preparedness among area residents. Monthly meetings of the committee are open to emergency management and municipal professionals, volunteers, and interested citizens. The committee oversees major projects, such as installing an advisory radio station and outdoor warning siren system, coordinating disaster preparedness seminars, and organizing monthly programs to disseminate disaster preparedness information to the general public. In recognition of its work on this issue, Tullahoma received an Excellence in Municipal Government Award from the Tennessee City Management Association.

Resources

City Response to Terrorism and Disaster. Lexington, KY: Kentucky League of Cities. 2002. www.klc.org/terrorism2.htm [2002-SEP-06].
This guide provides step-by-step advice on how to create and maintain a comprehensive emergency management program and includes the steps in the planning process, emergency management considerations, and hazard-specific information.

Community Response to the Threat of Terrorism. Fairfax, VA: Public Entity Risk Institute. November 2001. http://www.riskinstitute.org/ptrdocs/CommunityResponse-Terrorism.pdf [2002-AUG-15].
This collection of papers provides practical ideas on local government emergency preparedness.

"Emergency Preparedness and Response." (July 2002). The White House. www.whitehouse.gov/homeland/book/sect3-5.pdf [2002-AUG-22].
A chapter from the National Strategy for Homeland Security, this document discusses a variety of steps the federal government must take to plan and prepare for large-scale terrorist incidents, including support for local first responders.

"Emergency Readiness Issues Intersection." Washington, DC: International City/County Management Association. http://icma.org/issueintersections/er.cfm [2002-AUG-15].
This Web page contains links to dozens of documents on planning for emergency situations, including sample plans from cities across the United States.

Guide for All-Hazard Emergency Operations Planning: State and Local Guide (101). (September 1996). Federal Emergency Management Agency. www.fema.gov/rrr/gaheop.shtm [2002-AUG-26].
This document is a comprehensive guide to emergency planning for local officials.

Guide for All-Hazard Emergency Operations Planning: State and Local Guide (101) Chapter 6, Attachment G -- Terrorism. (September 1996). Federal Emergency Management Agency. www.fema.gov/rrr/allhzpln.shtm [2002-AUG-26].
The purpose of Attachment G is to aid state and local emergency planners in developing and maintaining a Terrorist Incident Appendix (TIA) to an Emergency Operations Plan (EOP) for incidents involving terrorist-initiated weapons of mass destruction (WMD). Find the entire Guide at www.fema.gov/pdf/rrr/slg101.pdf.

LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan. (August 2001). U.S. Environmental Protection Agency. www.epa.gov/ceppo/factsheets/lepcct.pdf [2002-AUG-22].
This document addresses the increased threats of biological or chemical terrorism in the U.S. and what local environmental planning committees (LEPCs) can do to prepare for and respond to them.

"Managing the Threat of Terrorism." Washington, DC: International City/County Management Association. ICMA IQ Report. December 2001.
This report explores what communities can do to prevent, prepare for, and respond to terrorist attacks—using both traditional and nontraditional methods of dealing with disasters

National Strategy for Homeland Security. (July 2002). The White House. www.whitehouse.gov/homeland/book/nat_strat_hls.pdf [2002-AUG-22].
The purpose of this document is to organize and mobilize the nation to secure the U.S. from terrorist attacks. This is a printable version of the entire 90-page report. Individual chapters of the report may be accessed at www.whitehouse.gov/homeland/book/index.html [2002-AUG-22].

"Oklahoma City - Seven Years Later: Lessons for Other Communities." Oklahoma City, OK: Oklahoma City National Memorial Institute for the Prevention of Terrorism. 2002.
Chapter 3 focuses on local and state government planning for and response to terrorist incidents.

"Organizing for a Secure Homeland." (July 2002). The White House.
www.whitehouse.gov/homeland/book/sect2-2.pdf [2002-AUG-22].
A chapter from the National Strategy for Homeland Security, this document discusses local governments' roles in homeland security efforts and coordination among all levels of government.

"Preparing for Terrorism: What Every Manager Needs to Know" by Howard Levitin. Washington, DC: International City/County Management Association. Public Management. December 1998.
http://icma.org/documents/index.cfm?code=%2A%2B%40%5C%23WUDM75%3C%2AGM%20%2A%0A&hdr=II [2002-AUG-15].
This pre-9/11 article discusses the reasons for implementing an emergency plan, and suggests first steps toward preparedness.

"Terrorism in America: Seven Preventative Steps for Every Municipal Employer" by Mark J. Neuberger. Washington, DC: International Municipal Lawyers Association. Municipal Lawyer. May/June 2002.
This article emphasizes the importance of a disaster recovery plan in your city and the necessary steps to develop it.

Terrorism Program Guide (draft). Falls Church, VA: International Association of Emergency Managers. March 2002. www.iaem.com/terrorism_program_guide_.html [2002-AUG-15].
This draft document offers detailed information on emergency planning, including organizing and setting priorities to develop a plan.

"What is Being Done to Protect the Nation's Water Infrastructure?" U.S. Environmental Protection Agency. www.epa.gov/safewater/security/index.html [2002-AUG-22].
This page provides links to security strategies for small/medium water utilities, grants for publicly-owned drinking water utilities, vulnerability assessment resources, and training resources.

2. Practice

Practice is the only way to implement and test your city's emergency plan. Not only does it make the plan a part of your everyday business, but also it is a practical and efficient way to identify and resolve procedural difficulties while always striving to improve the plan. Practice also can provide responders and management with a unique opportunity to learn how best to integrate the actions of multiple departments and intergovernmental organizations.

The key to making practice pay off for your city or town is to seek out opportunities to test your plan in as many ways as possible, at all levels of your government. Everyone who works for the city should at some point be part of the testing, with a special focus on first responders and managers of all city departments.

Practice's Many Forms. A guide to hometown security planning produced by the Kentucky League of Cities and the NewCities Foundation (http://www.klc.org/terrorism2.htm) provides information on a variety of ways to test your city's plan:

Orientation and education sessions: These are regularly scheduled discussion sessions to provide information, answer questions, and identify needs and concerns.

Tabletop exercises: Members of the emergency management group meet in a conference room setting to discuss their responsibilities and how they would react to emergency scenarios. This is a cost-effective and efficient way to identify areas of overlap and confusion before conducting more demanding training activities.

Lessons from the Working Group on Homeland Security

- Practice, practice, practice. *Planning + Practice = Performance*
- Emphasize training and cross-training for all personnel.
- Respond only with the necessary people on site so that other operations can be sustained.

Walk-through drills: The emergency management group and response teams actually perform their emergency response functions. This activity generally involves more people and is more thorough than a tabletop exercise.

Functional drills: These drills test specific functions such as medical response, emergency notifications, warning and communications procedures, and equipment, though not necessarily at the same time. Personnel are asked to evaluate the systems and identify problem areas.

Evacuation drills: Personnel walk the evacuation route to a designated area where procedures for accounting for all personnel are tested. Participants are asked to make notes as they go along of what might become a hazard during an emergency, e.g., stairways cluttered with debris, smoke in the hallways. Plans are modified accordingly.

Full-scale exercises: A real-life emergency situation is simulated as closely as possible. This exercise involves local emergency response personnel, employees, management, and community response organizations (see city examples below).

Training Issues. Training will be an essential element of your city's efforts to practice its plan for responding to a possible terrorist attack. Cross-training, particularly for first responders, is of special importance. In addition, by providing cross-training for responders in other fields on topics such as law-enforcement procedures, fire, rescue, HAZMAT, and weapons of mass destruction, you can make sure that all of the key players have the knowledge and experience to respond appropriately in many situations.

Fortunately, training is one area where the federal government provides considerable assistance. Below you will find links to a number of training resources from the federal government and others. In addition, please refer to the NLC document, *Homeland Security: Federal Resources for Local Governments*, Appendix C, for a comprehensive list of federal government training courses currently available.

Examples

Fort Lauderdale, FL (Population: 152,397). Fort Lauderdale offers a free seven-week training course for its Community Emergency Response Team (CERT). The purpose of the CERT effort is to create teams of citizens within neighborhoods that can provide immediate emergency response in the event of a disaster. Prior to the arrival of professional emergency responders, CERT participants can initiate disaster response and rescue skills learned in the training course. Such skills include basic fire suppression, basic first aid, and light search and rescue. Between 1996 and 2002, Fort Lauderdale trained more than 500 citizens for CERT.

Newark, NJ (Population: 273,546). Newark conducted a full-scale chemical warfare drill as part of the federal Domestic Preparedness Program. The drill simulated an attack on a local roller rink. Volunteer victims were given appropriate decontamination treatment from firefighters and emergency medical workers. The exercise was designed to enhance the capability of emergency responders, at all levels of government, to deal with the aftermath of biological, nuclear, or chemical terrorist attacks.

Glendale, CA (Population: 194,973). Glendale held a disaster drill in which a mock pipe bomb containing hazardous chemicals was disarmed, and 1,600 people were safely evacuated from a high-rise building. Forty city agencies were involved in the drill, which also included the decontamination of 200 victims and the apprehension of a suspect. The exercise was part of a grant program from the U.S. Department of Justice's Domestic Preparedness Program.

Idaho County, ID (Population: 15,511). Grangeville and other jurisdictions in Idaho County simulated a bioterrorist attack at the county airport. During the drill, local government agencies worked together and with state and federal agencies to effectively respond to the situation. Also involved were local hospitals, where victims were transported, and relief agencies such as the Red Cross. As part of the exercise, police apprehended a suspect.

Broken Arrow, OK (Population: 74,859). Broken Arrow staged a mock terrorist incident as a disaster preparedness exercise. The scenario included a break-in at the local water treatment

plant, and a fax to a local television station with the words "Death to America." The exercise also assumed that an outdoor concert with 75,000 attending was taking place in the city. The city police department and communications office worked together to decide how to respond as events unfolded.

Resources

"Comprehensive Exercise Program." Federal Emergency Management Agency. www.fema.gov/rrr/cepnew.shtm [2002-AUG-26].
Through training and disaster drills, the Comprehensive Exercise Program (CEP) improves the proficiency of federal, state, and local governments to perform emergency management functions in an efficient and timely manner.

"Education and Training." Federal Emergency Management Agency. www.fema.gov/tab_education.shtm [2002-AUG-26].
FEMA provides many programs, courses, and materials to support emergency preparedness and response for emergency personnel as well as the general public.

"Emergency Responder Guidelines." (August 1, 2002). U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/docs/EmergencyRespGuidelinesRevB.pdf [2002-AUG-22].
Intended for first responders, this document provides baseline information on the training necessary to respond to an act of terrorism using weapons of mass destruction.

"Emergency Response to Terrorism: Self-Study (ERT:SS) (Q534)." Federal Emergency Management Agency. www.usfa.fema.gov/dhtml/fire-service/nfa-off3ss2.cfm [2002-AUG-26].
This page provides access to a free, 10-hour, self-paced course designed to provide basic awareness training to prepare first responders for terrorist incidents. Students who successfully complete the exam will be eligible for a National Fire Academy certificate of training.

"Equipment Acquisition Grants." U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/grants/goals.htm [2002-AUG-22].
This page describes the ODP Equipment Grant Program, which provides funding to enhance the capacity of state and local jurisdictions to respond to incidents of domestic terrorism using weapons of mass destruction.

"Exercises." U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/exercises/state.htm [2002-AUG-22].
This page describes the ODP's State and Local Domestic Preparedness Exercise Program and aids states and local jurisdictions in advancing domestic preparedness through evaluation of authorities, plans, policies, procedures, protocols, and response resources.

"National Fire Academy." Federal Emergency Management Agency. www.usfa.fema.gov/dhtml/fire-service/nfa.cfm [2002-AUG-26].
This page provides links to courses and programs offered by the National Fire Academy (NFA). The NFA works to enhance the ability of fire and emergency services and allied professionals to deal more effectively with fire and related emergencies.

"ODP Weapons of Mass Destruction Training Program Course Catalog." U.S. Department of Justice, Office for Domestic Preparedness.
http://www.ojp.usdoj.gov/odp/docs/coursecatalog.pdf [2002-AUG-22].
This catalog is designed to provide emergency response personnel with comprehensive information regarding training courses and technical assistance offered by ODP.

"Overview: Training and Technical Assistance." U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/ta/overview.htm [2002-AUG-22].
This page describes the ODP's State and Local Domestic Preparedness Training and Technical Assistance Program and provides links to more detailed information. The program provides direct training and technical assistance to state and local jurisdictions to enhance their capacity and preparedness to respond to domestic incidents.

"Symposium Center/About PERI Symposium Programs." Public Entity Risk Institute.
www.riskinstitute.org/symposium.asp [2002-AUG-26].
This site lists the Public Entity Risk Institute's symposiums and issue papers, which are designed to provide municipal officials with information on risk assessment and emergency planning.

3. Communicate

Municipal leaders can play a crucial role in local efforts to prevent or respond to a terrorist attack simply by communicating effectively with the public and other key audiences. Both in the current climate of elevated risk and during an actual emergency event, local leaders are the most direct source of information for citizens in their cities and towns.

What People Want and Need to Hear. What does the general public want and/or need to know in these types of situations? They want to know what is happening, where to get assistance, whether to evacuate (and how), what other actions they should take, and where to get official information. They also want to be reassured that people are on top of the situation and that things are not spiraling out of control.

As was shown in the aftermath of the September 11 attacks, reassurance from senior government officials is critically important. Anthony Williams, Mayor of Washington, D.C., has suggested that a terrorist attack is unlike a typical emergency in that people need to have information and reassurance immediately. Gathering all the facts before reporting to the public is often not possible in a terrorist scenario. There are too many uncertainties, too much we still don't know. It is imperative that officials establish an immediate presence and provide as much information as possible.

Lessons from the Working Group on Homeland Security

- Engage citizens in new ways as part of the planning process.
- Focus on effective communications to ensure effective emergency preparedness, response, and recovery.
- Build strong working relationships well before an emergency.

Of course, the last thing local elected officials should do is go before the public with unsubstantiated theories and advice that has not been properly thought through. The key to successful communication is providing accurate and timely information, and that means building relationships with city staff, other local governments, state and federal officials, and others who can give you reliable information about what's happening and sound advice about what local residents should do.

Working with the Media. The media will be a crucial player in your efforts to communicate with the community about preparing for and responding to a crisis. Your relationship with the media requires continuous cultivation of key reporters, editors, producers, and more. These and other media representatives must understand your role, the city's role, and the roles of other entities in an emergency situation. It is important that they look to you as a partner in delivering accurate and relevant information to the public.

In the same way, local elected officials need to view the media as a partner. During an emergency, the media will be the primary source of information for the public about what's happened and how to respond. They need good information from you so they can convey it to the general public.

A variety of resources are available for local elected officials seeking to work more closely with the media on emergency preparedness and other issues. For example, NLC's Leadership

Training Institute offers courses on media relations for local elected officials. For more information, go to www.nlc.org/nlc_org/site/programs/training_and_education/index.cfm. In addition, the International City/County Management Association (ICMA) provides information on media relations in emergency situations on the Web at www.icma.org/issueintersections/dsp_ER.cfm?SubCategory_Name=Media%20Relations%20in%20Emergency%20Situations.

What to Communicate in an Emergency Situation

- Official incident information
- Available local and state public resources
- Private resources
- Capabilities of neighboring jurisdictions
- Federal resources
- Status reports
- Local and state resources deployed
- Emergency public information
- Where to go for official information

Source: *IAEM Terrorism Program Guide*, International Association of Emergency Managers (see www.iaem.com/Emergency_Response_Info.doc).

Engaging Citizens. The news media, of course, is not the only conduit to reach out to the public. Cities can develop newsletters, flyers, and special reports for direct distribution to city residents through the Internet, telephone, or by mail (see examples below from Sugar Land and San Antonio, TX, and East Haven, CT).

A key step in local officials' efforts to communicate with citizens about disaster-related issues is to first gauge public opinion and sentiment on the topic. What are the priorities of local residents? What do they need to feel safe and secure in their community? As an elected official, you are constantly taking the pulse of your constituents, but sometimes it is important to consider using more systematic ways of gathering information, such as citizen surveys, meetings with civic leaders, or town hall meetings (see examples from Daytona Beach Shores, FL, and Columbia City, OR). With a better idea of what people are thinking and what their true concerns are, you will be better able to communicate with them more effectively.

Special public meetings on homeland security issues can be an especially effective tool for both gauging public opinion and disseminating important information. The meetings may focus on any number of topics, from emergency preparedness to disaster response to grieving in the aftermath of an emergency event (see example from Roseville, MN).

One type of public meeting that many cities have found particularly effective is a "study circle." A study circle is a small group of people from different backgrounds and viewpoints who meet several times to talk about an issue. The Study Circles Resource Center developed a discussion guide for study circles titled "Facing the Future: How Should We Move Forward After September 11?" Find it at www.studycircles.org/pages/issues/americaresponds.html.

Another way to engage citizens is to encourage volunteerism with local organizations. For those individuals who are interested specifically in community safety, the National Crime Prevention Council (http://www.ncpc.org) provides information on Neighborhood Watch programs. In addition, the federal government has been encouraging citizen volunteerism with Citizen Corps. This component of the federal program, USA Freedom Corps, creates opportunities for all citizens to participate in making their communities safer and better prepared for preventing and

handling threats of terrorism, crime, and disasters of all kinds. You can learn more about Citizen Corps at http://www.citizencorps.gov/

In the Event of an Emergency. In the event of an emergency, local officials must be prepared to communicate not only with the general public but also with incident commanders, first responders, and state and federal government agencies. A good resource for further information on preparing for communications in an emergency situation is the "IAEM Terrorism Program Guide" from The International Association of Emergency Managers (see www.iaem.com/Emergency_Response_Info.doc).

First responders are just a few of the nodes in a complex communications network that includes city departments (police, fire, and EMS among the most critical), as well as other local governments in the area, state and federal agencies, and quasi-public and private entities such as utilities that provide essential services. Effective communication with all of these key players requires more than a clear and consistent message; it requires clear and unambiguous channels of communication. This means local elected officials need to pay special attention to the issue of compatibility, or interoperability, among communications systems, equipment, and frequencies.

Examples

Washington, DC (Population: 572,059). To ensure interoperability in the Washington area, the Metropolitan Washington Council of Governments (COG) developed a communications infrastructure component as part of its Regional Emergency Coordination Plan. COG brought together communications and IT experts from regional organizations, area local governments, state and federal government communications organizations, and private sector communications providers to draft the document. Find the document at www.mwcog.org/homeland_plan/download/RESF02_10%20April.pdf.

Sugar Land, TX (Population: 63,328). Shortly after September 11, Sugar Land committed to enhancing public communication about emergency planning. The city mailed flyers to every home, offering information on homesite emergency planning. The flyer included a hotline number residents can call during an emergency to obtain the most current critical information. The flyer can be downloaded from the Web at www.ci.sugar-land.tx.us/preparation/EmergPrep.pdf (June 20, 2002. *Houston Chronicle*. "Sugar Land tries to alert residents to procedures during emergencies")

San Antonio, TX (Population: 1,144,646). When San Antonio was hit with massive flooding in July 2002, it used its Website to provide up-to-the-minute information on road closures, evacuations, FEMA assistance, and helpful hints for residents seeking contractors to repair damaged homes. The city maintained the site weeks after the flood subsided, focusing on flood relief information.

East Haven, CT (Population: 28,189). East Haven uses a "reverse 911" system to contact residents in the event of a citywide emergency. The automated system can make 1,000 emergency calls in one hour, to regular or cell phones, in- or out-of-state. Before installing the system, emergency workers would drive through the streets with loudspeakers, and could reach only 50 residents per hour. The $22,000 system was paid for by Project Impact funds from the Federal Emergency Management Agency (FEMA).

Daytona Beach Shores, FL (Population: 4,299). Citizens of Daytona Beach Shores participated in a community forum designed to assist city leaders with long-range planning for an emergency management program. The result was a set of emergency operations plans and the development of an emergency operations center.

Columbia City, OR (Population: 1,571). Columbia City surveyed its citizens to obtain information about residents' needs and their abilities to help others in case of a Y2K emergency. The first portion of the city's questionnaire asked citizens if they thought they would need assistance in the event of an emergency. The second portion asked for volunteers to assist other residents by helping in an emergency or checking on their well-being.

Roseville, MN (Population: 33,690). Roseville hosted a community emergency readiness night in June 1999. The presentation and discussion, open to all citizens, answered questions about how residents can prepare their homes for all types of severe weather, as well as Y2K problems. Residents also learned how their city and county were preparing for possible Y2K-related disruptions to government services and equipment. Presenters at the meeting included representatives from the city, Ramsey County, the Red Cross, the local power provider, and a medical systems organization.

Denver, CO (Population: 554,636). The Rocky Mountain Center for Medical Response to Terrorism, Mass Casualties, and Epidemics is a project that gives Denver city officials and doctors at area hospitals a venue for responding to emergency medical situations. Part of the Center plan includes the upgrade of a phone system that, in the event of a catastrophic event such as a bioterrorism attack, can handle up to 1,000 calls a day from worried citizens. The $50,000 upgraded system would provide options for the masses of people who might otherwise go to area emergency rooms to have their questions answered. Plans call for the Center to provide public education seminars about bioterrorism and convene hospital officials to discuss cooperative efforts in treating mass casualties.

Lake County, OH (Population: 227,511). Designed especially for use during emergency events, Lake County's mixed-mode voice communications system provides interoperability among area municipalities and the county. All 40 local police, fire, and EMS departments are connected to the system, as well as 25 public service agencies and all area schools. Incorporating a mix of digital and analog technologies, the system uses more than 1,100 mobile radios, 85 control stations, and an eight-position dispatch console. It is also compatible with the radio system used in neighboring Geauga County.

Resources

"Emergency Readiness: Citizen Guides" International City/County Management Association. www.icma.org/issueintersections/dsp_ER.cfm?SubCategory_Name=Citizen%20Guides%20for%20Emergency%20Preparedness [2002-AUG-26].
This collection of citizen guides for emergency preparedness includes 20 examples, most of them developed by local governments.

"Emergency Readiness: Media Relations" International City/County Management Association. www.icma.org/issueintersections/dsp_ER.cfm?SubCategory_Name=Media%20Relations%20in%20Emergency%20Situations [2002-AUG-26]
This page provides information on media relations in emergency situations for local governments.

"Emergency Response Information." International Association of Emergency Managers. www.iaem.com/Emergency_Response_Info.doc [2002-AUG-26].
IAEM presents ideas on emergency response information and communication in its working document, "IAEM Terrorism Program Guide."

"Facing the Future: How Should We Move Forward After September 11?" Study Circles Resource Center. www.studycircles.org/pages/issues/americaresponds.html [2002-AUG-26].
This site promotes the benefits of engaging citizens in discussions about homeland security through study circles. A study circle is a small group of people from different backgrounds and viewpoints who meet several times to talk about an issue.

"Field Office Information." Federal Bureau of Investigation. www.fbi.gov/contact/fo/info.htm [2002-AUG-22].
This page provides links to FBI field offices in cities across the country. The list is sorted alphabetically by city name.

Guide for All-Hazard Emergency Operations Planning: State and Local Guide (101) Chapter 5, Attachment B -- Communications. (September 1996). Federal Emergency Management Agency. www.fema.gov/pdf/rrr/5-ch-b.pdf [2002-AUG-26].
The purpose of Attachment B is to provide details necessary for understanding total emergency communications plans. Find the entire Guide at www.fema.gov/pdf/rrr/slg101.pdf.

"Homeland Security State Contact List" The White House. www.whitehouse.gov/homeland/contactmap.html [2002-AUG-22].
A clickable map lets you select your state to see whom the governor has appointed as the homeland security contact.

"Information Sharing and Systems" (July 2002). The White House. www.whitehouse.gov/homeland/book/sect4-2.pdf [2002-AUG-22].
A chapter from the National Strategy for Homeland Security, this document discusses integrating communications and information sharing among all levels of government and the private sector. It also calls for adopting data standards.

"Leadership Training Institute." National League of Cities. www.nlc.org/nlc_org/site/programs/training_and_education/index.cfm [2002-AUG-2002]
NLC's Leadership Training Institute offers courses on media relations for local elected officials.

"National Crime Prevention Council." Washington, DC: National Crime Prevention Council. www.ncpc.org [2002-SEP-06].
This is the home page of the organization and includes links to community-based prevention programs, ideas for neighborhood action, and a crime prevention library.

"National Crime Prevention Council: Neighborhood Action." Washington, DC: National Crime Prevention Council. www.ncpc.org/neigh.htm [2002-SEP-06].
This page has a variety of links to information on topics like citizen patrols, involving youth, multiculturalism, neighborhood watches, and reaching out to crime victims.

United for a Stronger America: Citizens' Preparedness Guide. (January 2002). Washington, DC: National Crime Prevention Council. www.weprevent.org/usa/cover.pdf [2002-SEP-06].
This guide provides suggestions for citizens on preparedness in their homes, neighborhoods, schools, workplaces, places of worship, and public areas.

4. Prepare Your Local Government

At the same time that you are working to make sure your community as a whole is ready to respond to a terrorist attack, you, as a local elected official, also must make sure the government itself is ready. More than anything else, that means planning for the protection of city employees and the continuation of your city government. It also means paying close attention to issues of liability and insurance.

Employee Evacuation and Support. Your city's employees are your most important resource. As part of your overall emergency plan, you will need a well-defined set of procedures for city employees to follow in the event of an attack. Priorities include the development of a coordinated evacuation plan for all city buildings, as well as plans and guidelines for providing critical support to city employees in the aftermath of a disaster.

Lessons from the Working Group on Homeland Security

- Plan for continuity of government during and after an emergency.
- Consider the human element of employee response.
- Respond only with the necessary people on site so that other operations can be sustained.

Evacuation. A well-prepared emergency evacuation plan for city buildings should do the following:

- Outline the responsibilities of the building safety supervisor, such as preparing a building diagram, determining building occupancy, assigning a method to announce an evacuation, assigning evacuation team members, and scheduling fire drills.
- Outline the responsibilities of other team members, as well as individuals who are not on the evacuation team, and establish a chain of command.
- Describe evacuation routes and procedures for staff and patrons, as well as staff guidelines for ensuring the evacuation of all occupants from the building
- Provide instructions for those unable to evacuate independently because of physical or mental conditions.

Several sample evacuation plans are described in the examples below (see Montgomery County, MD, and Gresham, OR).

Support. It is natural that city employees will deal with emotional issues in the aftermath of a disaster. No one who witnesses or is directly affected by such an event is untouched. Victims, witnesses, and first responders may all struggle with emotions ranging from profound anger to sadness and grief.

At the same time, people directly affected by a disaster often do not see themselves as requiring mental and physical health services; as a result, they may be unlikely to request them. This means your local government will need to do more than simply distribute

information about available services. Outreach may be necessary to make sure that critical services reach everyone who needs them.

Municipal governments should negotiate pre-planned interagency agreements with local health service facilities so that victims of a disaster can receive immediate, short-term crisis care and counseling, as well as ongoing support. Grants to provide counseling and education for individuals affected by disasters are available to states through the Center for Mental Health Services (working in collaboration with the Federal Emergency Management Agency). Visit their web site to read more about dealing with the emotional aftermath of a disaster: www.mentalhealth.org/cmhs/emergencyservices/after.asp

Continuity of Government. Planning for continuity of local government in the event of a crisis is essential. Your city's plans should be directed at ensuring that government can continue to perform essential functions, with key communications and other systems intact, while also coordinating the local recovery effort. Important issues to consider include: planning for possible alternate sites for the center of government; establishing a clear chain of command and lines of succession (including boilerplate delegations of authority); and planning for the off-site preservation of computerized and paper records, including such items as ordinances, resolutions, deeds, tax records, and building permits.

Risk Analysis. Risk analysis is an important first step to protecting your city in the event of a terrorist attack. It is a task that should be completed even before you develop an emergency plan. Your job is to identify and analyze risks, including potential loss and impact summaries, and then to develop a plan to control and mitigate those risks. Your plan should be able to be used both on a citywide basis and to identify and analyze risks in specific areas or operations.

To conduct the risk analysis, your emergency planning team should use questionnaires, on-site, in-depth data gathering, and other methods to pursue a rigorous identification of all risks and environmental issues in your city. As a resource, the National Center for Small Communities is preparing a risk management primer that will cover risk management needs, a community risk management checklist, types of insurance coverage available, and what the insurance does and does not cover. This primer will be available late fall 2002 on the Center's website, www.smallcommunities.org

Insurance and Liability Issues. A crucial part of managing a city's risks is deciding how to cover the costs of emergencies that the city cannot avoid, reduce, control, or transfer to others. To make an informed decision, a city must first identify its risk financing needs, and then assess its ability to meet those needs.

By identifying financial risks, you can protect your city from unknowingly retaining financial responsibility for potentially catastrophic losses. Equally important is a careful review of the city's insurance policies. Considering that terrorism insurance is now either unavailable or prohibitively expensive, cities need to identify and analyze their risks to determine exactly what kind of losses they can sustain.

State leagues may provide a possible option for some cities. More than 33 state municipal leagues have developed and sponsored intergovernmental risk-sharing pools. These

arrangements can help to shield cities and towns from the traditional insurance market's cyclical problems of cost, capacity, and uncertainty. In addition to contacting your state league, you may want to visit the website of the Risk Management Resource Center for additional information about risk and insurance issues for cities. The site (www.eriskcenter.org/statelocal/department/dept_ddi.html) provides links to the insurance regulation departments of all 50 states.

Examples

Gresham, OR (Population: 90,205) To ensure a safe work environment for city employees, Gresham, OR published evacuation procedures for city facilities. The document provides instructions on how to safely exit buildings and other facilities in the event of an emergency. It is divided by type of emergency: fire, hazardous materials, explosion, armed or dangerous intruder, and earthquake. Maps of each floor of each city facility, including city hall, are included in the plan, as is a notification/call tree diagram. The evacuation plan also provides detailed instructions for persons with disabilities and those who may assist them in an emergency situation. Find the complete document on the Web at http://icma.org/documents/index.cfm?code=%2A%2A%40%5C%21VU%2CO74%5C%3AE%3AP%2C%0A&hdr=II [2002-SEP-03].

Stoughton, MA (Population: 27,149) Stoughton, MA, school officials developed a user-friendly handbook for teachers and staff to use in case of emergency. Developed by a committee with input from police and fire departments, the guide covers crisis scenarios such as fires, natural disasters, and utility malfunctions. It provides emergency telephone numbers and the appropriate immediate response and steps to follow in each situation. Designed in a flip chart format to allow all topics to be seen at once, the guide is customized for each of the town's schools with building maps, evacuation procedures, phone numbers, and crisis management teams.

Montgomery County, MD (Population: 873,341) Montgomery County, MD developed a step-by-step guide for developing a building evacuation procedure. The guide stresses the importance of having a safety supervisor and floor wardens in each building to oversee the evacuation process, and especially for making sure that persons with disabilities and others requiring assistance are helped. The guide also details other roles including those of assistant floor wardens, searchers, alternates, persons who first discover the emergency situation, and all others who are not assigned a specific task. Find the complete document on the Web at http://icma.org/documents/index.cfm?code=%2C%2A%40%5C%23V5LO10E0%40WB%3F%0A&hdr=II [2002-SEP-03].

Resources

"Disaster Mental Health: Tips for Talking About Disasters." U.S. Department of Health and Human Services. www.mentalhealth.org/cmhs/emergencyservices/after.asp [2002-SEP-03]. This Web page provides links to sites that focus on disaster mental health for adults, children, and disaster response workers. It also links to Spanish-language sites.

"Facing the Future: How Should We Move Forward After September 11?" Study Circles Resource Center. www.studycircles.org/pages/issues/americaresponds.html [2002-SEP-03].
This site promotes the benefits of engaging citizens in discussions about homeland security through study circles. A study circle is a small group of people from different backgrounds and viewpoints who meet several times to talk about an issue.

"Needs Assessment and Strategy Development." U.S. Department of Justice, Office for Domestic Preparedness. https://grants2.ojp.usdoj.gov/servletext/OS_localJur_index [2002-AUG-22].
Local governments may download the "Assessment and Strategy Development Toolkit" from this page. Assessments ensure that measures taken to reduce vulnerabilities are justifiable and that ODP grants are appropriately targeted to address identified risks and requirements.

"Planning for Disaster Recovery." The International City/County Management Association (ICMA). First printed in 1993, this 24-page report provides case studies of the disaster recovery process and discusses problems, resources, and solutions. The report is still available—call ICMA at 800-745-8780 and ask for item #40834.

"Risk Management Primer for Small Town and Township Officials." Public Entity Risk Institute. www.riskinstitute.org/project.asp?item_id=1006 [2002-SEP-03]
Scheduled for release in late fall 2002, this primer is designed to introduce small town leaders to key considerations in managing overall risks in their jurisdictions. It includes a community risk management checklist, types of insurance coverage available, and what the insurance does and does not cover. The primer was developed by the National Center for Small Communities, through a project funded by a grant from PERI. The primer will be available on the NCSC website, www.smallcommunities.org.

"State Departments, Divisions of Insurance." Risk Management Resource Center. www.eriskcenter.org/statelocal/department/dept_ddi.html [2002-SEP-03].
This site provides links to the insurance regulation departments of all 50 states.

5. Aggressively Seek Funding—Find and Use Resources

Federal Resources. In addition to the multiple resources found in this document, please refer to NLC's *Homeland Security: Federal Resources for Local Governments*. This reference guide is posted on NLC's website as a working document to provide local elected officials with the latest information on the programs and resources available at the federal level to help municipalities prepare for and respond to threats of terrorism. Like this document, it will be updated on a regular basis to provide the latest information on federal resources to support local efforts to insure homeland security.

The goal of *Homeland Security: Federal Resources for Local Governments* is to guide municipal officials through the maze of federal efforts, programs, and funding that deal with this subject. In addition to explaining the current structure of federal initiatives, the report outlines how state and federal agencies can assist local preparedness efforts in five key areas: planning; training and exercises; equipment; intelligence; and health issues. Last, but not least, the report lists important resources to help cities prepare for and report terrorist attacks, along with training courses available across the country for first responders and incident managers.

PART TWO: KEY ISSUES

As part of its effort to serve as a front-line resource on terrorism for local elected leaders, the National League of Cities (NLC) Working Group on Homeland Security has identified a number of key issues that officials should know about and keep in mind as they plan their communities' responses to terrorism. In the following pages, we provide perspective on seven of these issues, as well as resource links. This discussion builds on the broad overview of local officials' roles in ensuring hometown security that we presented in Part One of this document.

The key issues covered in Part Two fall into two broad categories, as follows:

Be Aware. Local elected officials need to be able to assess the threat to their cities and towns—whether it is a conventional attack, an attack with chemical, biological, or radiological weapons, or a cyberterror attack. Only by understanding the different types of attacks and what they might entail can local leaders plan how best to prepare their communities.

Be Prepared. Preparing for a possible terrorist attack on your city or town means taking action on a wide range of fronts. Among the most important things you can do is to ensure that first responders have the ability to communicate effectively across agencies and levels of government, that all key people are sufficiently trained, and that local government is prepared to communicate in a crisis.

In addressing each of the key issues in this section, we have divided the discussion into two parts: "At Issue," which includes general information about the issue and why it is important; and "Ideas for Local Action," which provides helpful guidance and resources for local elected officials about how to deal effectively with the issue in question. The key issues are:

1. **Attacks with Conventional Explosives**
2. **Bioterrorism**
3. **Nuclear and Radiological Attacks**
4. **Cyberterrorism**
5. **Interoperability**
6. **Training**
7. **Crisis Communication**

Share Your Experiences. The NLC Working Group on Homeland Security welcomes examples and case studies from cities and towns throughout the country that are working on these issues and can share their "lessons learned" with others. Please contact a member of the Municipal Reference Service staff here at NLC at (202) 626-3130 or at mrs@nlc.org. We look forward to sharing these stories in the weeks and months ahead as part of the Working Group's continuing efforts to update and expand on the information presented in this document.

1. Attacks with Conventional Explosives

Local officials and law enforcement should remember that the most likely type of terrorist weapon is a conventional explosive device, even as you prepare for biological, chemical, and radiological attacks.

At Issue

Conventional weapons pack a very powerful punch and can bring down large buildings; casualties can number in the hundreds, as they did when domestic terrorist Timothy McVeigh used a fuel oil-fertilizer bomb to attack the Murrah Federal Building in Oklahoma City.

Ideas for Local Action

While Part One of this document covered many aspects of planning for and responding to conventional attacks, here we offer some specific response guidelines from a hazardous materials expert. In a recent monograph prepared for the Disaster Preparedness and Emergency Response Association, Robert J. Heyer reflected on some of the issues that local authorities should consider in the immediate aftermath of an attack with conventional explosives:

- First responders should be alert to the potential for structure collapse as well as secondary explosive devices in the area.
- Great caution should be used if the explosion seems to do little damage. A small explosive device might be used to disperse chemical, biological, or even radioactive agents. Another purpose of a small device might be to bring large numbers of first responders, who are then subjected to a larger secondary device.
- Another immediate problem for responders and victims is the potential for asbestos exposure. Older buildings may contain asbestos as insulation, pipe coverings, siding or roofing, flooring, adhesives, floor or ceiling tile, and wall panels. Any explosion or collapse may cause this asbestos to become airborne in hazardous levels.
- Immediately, the primary inhalation threat and decontamination problem will be dust. Any expedient breathing protection should be used—masks, wet towels, handkerchiefs, etc.—while people exit the area immediately.
- Footbaths and wash-downs are most effective for decontamination of normal conventional incidents if asbestos exposure is suspected. Eye washing with clean water is usually needed immediately as well.
- In the event of an attack with an airplane, quantities of residual, unburned fuel may remain. In addition to the resultant fire hazard, aviation gasoline and jet fuel are hazardous substances, and decontamination efforts may need to include removal of the fuel contaminant.

For the complete monograph, see www.disasters.org/dera/library/Heyer%20WMD.pdf

Resources

Please see Part One of this document, for additional links related to attacks with conventional weapons.

2. Bioterrorism

A series of anthrax mailings in the fall of 2001 marked the first bioterror attacks on U.S. soil. They also highlighted the importance of the "golden triangle" of response between clinicians and clinical microbiologists, the health-care delivery system, and public health officials.

At Issue

Biological Agents. The Centers for Disease Control and Prevention (CDC) lists six biological diseases and agents as "Category A" threats. According to CDC, these high-priority agents include organisms that pose a risk to national security because they:

- Can be easily disseminated or transmitted from person to person;
- Result in high mortality rates and have the potential for major public health impact;
- Might cause public panic and social disruption; and
- Require special action for public health preparedness.

The CDC's category A agents include: anthrax; botulism; plague; smallpox; tularemia; and vital hemorrhagic fevers such as the Ebola virus. More information about each of these agents, as well as other biological threats, can be found at www.bt.cdc.gov/agent/agentlist.asp.

Delivery Methods. The Public Entity Risk Institute (PERI) lists the following terrorist-initiated scenarios that could intentionally expose citizens to biological agents:

1. *Bioaerosol development and dissemination via man-made delivery systems.* In this scenario, terrorists would use man-made systems such as HVAC or reservoirs to disseminate bioaerosols containing anthrax, botulinum toxin, or other agents. High-use community areas such as domed stadiums, shopping malls, subways, and governmental complexes would be prime targets.

2. *Hazmat incidents involving biomedical materials.* This category would include the intentional discard of medical wastes and infectious tissue material into or onto a target site. Substances would include human and/or animal tissue and blood samples of the type used in medical research. Considering that the health effect of these types of terrorist-initiated releases would be limited, the terrorists' primary objective in these cases would be to provoke public panic.

3. *Shipment of pathogens.* Packaging containing pathogens such as anthrax, botulism and plague are routinely shipped throughout the country from type collection laboratories to medical and microbiological research facilities. The concern for emergency responders is that a terrorist group, disgruntled graduate student, or angry medical researcher might target a shipment; intercept the package containing the bioagents; and use the contents as seed stock for biological weapons production. In addition, the placement of the stolen container at a high-use area would result in citizen trauma and panic.

4. *Use of biological agents for agricultural pest or public health pest control.* Equipment designed for dispersion of *Bacillus thuringiensis* (BT) to combat mosquitoes and black

flies could be easily adapted for bioaerosol dispersion of anthrax spores. In addition, BT formulations could be contaminated by anthrax and applied by air or ground spray equipment used in mosquito control and agricultural pest activities.

Of course, each community's risks are different. To identify and manage these risks, PERI recommends that local governments follow the basic risk management process of identifying the community's most likely vulnerabilities, evaluating its options for addressing those exposures within the bounds of the law, and then choosing and implementing the best options.

For more information: www.riskinstitute.org/lib_art.asp?art_id=1015

What About Chemical Weapons?

Experts consider biological weapons to be considerably more dangerous than chemical weapons, primarily because of the potential impact on large numbers of people. At the same time, however, chemical weapons were described in a recent *Time Magazine* article as "by far the most popular among terrorists." The reason: they are relatively easy to get, and the finished products don't have to be kept alive.

According to the Centers for Disease Control and Prevention, chemical agents fall into one of several categories defined by the effect of the agents on humans:

- Choking agents such as chlorine;
- Blood agents such as hydrogen chloride;
- Blister agents such as mustard gas;
- Nerve agents such as Sarin; and
- Incapacitating agents such as BZ.

Local response to a chemical attack would follow many of the same procedures as the response to bioterror and require the same level of coordination among public health officials, the health care delivery system, and others. For a complete list of chemical agents commonly found in weapons, as well as links to other information, see www.bt.cdc.gov/Agent/agentlistchem.asp.

Ideas for Local Action

Government Roles. The Public Entity Risk Institute identifies several roles for local governments in hardening their facilities and communities against biological attack:

- Governments can encourage the managers of potentially vulnerable private sites to secure and limit access to ventilation and water systems, install HEPA (high efficiency particulate air) filters in their HVAC systems where possible, and hire trained security guards to control building access. Governments also can and should take similar actions in public buildings.
- Governments can encourage (or require) promoters of public events to provide additional security for those events by hiring adequate numbers of security personnel who have been trained to recognize the signs of a possible biological terrorist attack.

- Governments can assess their internal procedures (such as mail handling and package receipt) for any weaknesses that might increase vulnerability to a bioterrorist attack, and can encourage other organizations in the community to do the same.
- Governments can educate citizens to be alert, and to report to the proper authorities potential problem behaviors that they observe, such as attempts to gain unauthorized access to secured areas.

For more information: www.riskinstitute.org/lib_art.asp?art_id=1025

Responding to a Crisis. Local health officials from Palm Beach County, FL, and Washington, D.C., two communities directly affected by the 2001 anthrax attacks, reflected on the lessons from the experience in a conference call hosted by the National Association of City and County Health Officials in November 2001. Among the lessons these front-line officials shared:

- As the first responder in any bioterror incident, the local health department needs to rapidly increase its ability to communicate effectively and efficiently with physicians, hospitals, and HMOs.
- Communication between the various response organizations and the media is critical, and authorities should have more than one method of communicating with the general public.
- Workshops and seminars for private providers and public health workers about issues pertaining to bioterrorism improve preparedness and allow for a prompt response.
- Syndromic surveillance systems are vital for early detection of unusual diseases and the ability to respond quickly to bioterrorism.
- Officials should address the challenge of creating and maintaining "surge capacity" at the local level.

For additional lessons learned and other information, see the conference call transcript at www.naccho.org/general456.cfm

A To Do List for Local Governments. In a July 2001 publication, *The Public Health Response to Biological and Chemical Terrorism: Interim Planning Guidance for State Public Health*, the Centers for Disease Control and Prevention (CDC) identified a series of fairly obvious roles for public health departments in planning and responding to bioterrorist attacks. These include:

1. Identify the types of events that might occur in their communities;
2. Plan emergency activities in advance to ensure a coordinated response;
3. Build the capabilities necessary to respond effectively to the consequences of those events;
4. Identify the type or nature of an event when it happens;
5. Implement the planned response quickly and efficiently; and
6. Recover from the incident.

Expanding on the CDC's advice, the Public Entity Research Institute offers the following suggestions of specific activities that local governments might want to undertake:

1. *Strengthen information and communications technology.* Be certain that the local public health department has the information and communications technologies it needs to respond effectively in a public health emergency. These include surveillance technology, e-mail, high-speed Internet access, fax capability, and reliable and secure alternative voice communication services such as radios.

2. *Strengthen working relationships and communications.* Strengthen the local health department's working relationships and communications capabilities with local community stakeholders and the health care community, and with the state health department and federal agencies. Examples of potential partners include: the Federal Emergency Management Agency (FEMA); the U.S. Environmental Protection Agency (USEPA); the Federal Bureau of Investigation (FBI); the U.S. Department of Justice; the Centers for Disease Control and Prevention (CDC); the state health department; state and local offices of emergency management; regional councils of government; neighboring local health departments; emergency medical services; hospitals; and primary care medical offices and clinics.

3. *Educate the health care and emergency response community about identification of bioterrorist attacks and agents.* Be certain that the local health care and emergency response community is familiar with possible biological agents that could be used in terrorist attacks; the signs and symptoms of infectious diseases most likely to be caused by those agents; appropriate disease surveillance procedures; the indications of a covert biological attack, such as an unusually large number of affected people with similar illnesses or the occurrence of an unusual illness; and the appropriate protocol for reporting unusual disease activity to local and/or state public health departments.

4. *Educate the health care and emergency response community about medical treatment and prophylaxis for possible biological agents.* Be certain that the local health care and emergency response community is familiar with the appropriate protocols for caring for victims of biological attacks and providing prophylaxis to people who were exposed but are not yet ill. Have written and current protocols readily available for reference.

5. *Educate the local health department about state and federal requirements and assistance.* Be certain that the local health department is familiar with the appropriate channels for reporting disease outbreaks to the state health department and requesting state and federal assistance with management of infectious disease outbreaks. (For emergency notification procedures from the CDC, see http://www.bt.cdc.gov/emcontact/index.asp)

6. *Maintain a locally accessible supply of medications, vaccines and supplies.* Be certain that the local health department knows which medications, vaccines, and supplies will be needed for each potential biological agent. Make certain the health department maintains, or has arrangements to immediately access, a stockpile of these materials in the event of an infectious disease outbreak.

7. *Address health care worker safety issues.* Be certain that public health workers and emergency responders are trained about transmission of infectious diseases and worker biosafety issues, and provide appropriate personal protective equipment and emergency

prophylaxis. Advance preparation for worker safety may help prevent needed health care workers from becoming ill or refusing to work during an epidemic.

8. *Designate a spokesperson to maintain contact with the public.* Identify a primary and back-up spokesperson to inform and reassure the public, interact with the news media, and provide educational materials to the public. Ensure that all spokespersons are well informed and familiar with state and local procedures.

9. *Become familiar with state and local laws relating to isolation/quarantine.* Be certain local officials are familiar with local and state health regulations restricting the movement of people exposed to communicable diseases.

10. *Develop, maintain and practice an infectious diseases emergency response plan.* Develop, regularly update, and practice a written infectious diseases emergency response plan that details the local government's plans for managing infectious disease outbreaks.

11. *Practice with surrounding jurisdictions.* Consider testing the infectious diseases emergency response plan by conducting a practice exercise with surrounding jurisdictions.

12. *Stay current.* Bioterrorism has become a front-burner issue in recent months; new developments come to light every day. As a result, local governments need to stay on top of the latest news and information so they can serve their communities as effectively and efficiently as possible.

Protecting Water and Food Supplies

Though experts believe the threat of chemical or biological attacks on the nation's water and food supplies is minimal, policy makers and utilities across the country are preparing for the possibility. In 2001, authorities in the United Kingdom spent $2.7 billion and killed 4 million animals to control foot-and-mouth disease, which is highly contagious but not harmful to humans. Whether intentional or not, a similar outbreak in the United States could shake Americans' faith in our traditionally safe and abundant food supply.

The introduction of microbiological agents to U.S. water supplies—whether at a reservoir, a treatment plant, or a water-distribution system—could pose an even greater health risk. For more on what states and localities are doing to address these threats, see "Bioterrorism: A Threat Without Borders," Council of State Governments, www.stars.csg.org/sgn/2002/february/0202sgn_18.pdf

Resources

"A National Teleconference on Bioterrorism: Lessons and Practices in Cooperative Planning for Bioterrorist Events." The Council on State Governments.
http://www.csg.org/bioterrorismteleconference.htm. [2002-OCT-25]
Transcript of a teleconference on state-local cooperation in addressing the threat of bioterrorism.

"Additional Resources [on Bioterrorism]." National Association of City and County Health Officials (NACCHO). http://www.naccho.org/general500.cfm. [2002-OCT-25]
Includes Articles, organizational links, training and coursework, and other resources.

"Bioterrorism and Local Public Health Case Examples from Recent Anthrax Events Summary." NACCHO. http://www.naccho.org/general456.cfm. [2002-OCT-25]
"Best Practices" examples from a discussion among local officials on dealing with the Anthrax situation following the Sept. 11 attacks.

"Bioterrorism-Related Anthrax." Centers for Disease Control and Prevention.
http://www.cdc.gov/ncidod/eid/index.htm. [2002-OCT-25]
Numerous articles on Anthrax detection, prevention, research.

"Bioterrorism – A threat Without Borders." Council on State Governments.
http://stars.csg.org/sgn/2002/february/0202sgn_18.pdf. [2002-OCT-25]
Key issues on bioterrorism preparedness, as well as model state homeland security initiatives.

"Cybercare." (July 2002). Journal of Homeland Security.
http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=69 [2002-OCT-25]
Presents a new strategy for mobilizing health care resources in the event of a bioterrorist attack.

"Disasters Present Health Challenges." (Oct. 2001). Council on State Governments.
http://stars.csg.org/sgn/2001/october/1001sgn23.pdf. [2002-OCT-25]
The impact of terrorism on the health care system and tips on how to be prepared.

"Early Warning and Remediation: Minimizing the Threat of Bioterrorism." (April 2002). Journal of Homeland Security.
http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=54 [2002-OCT-25]
Focuses on the early detection of biological agents used as weapons of mass destruction.

"Elements of Effective Bioterrorism Preparedness." National Association of City and County Health Officials. http://www.naccho.org/files/documents/Final_Effective_Bioterrism.pdf. [2002-OCT-25] Manual for Local Public Health Officials on how to prepare for a Bioterrorist attack.

"Emergency Response." CDC. http://www.bt.cdc.gov/emcontact/index.asp. [2002-OCT-25]
Describes who to contact in case of an act of bioterrorism or exposure to chemical/biological agents.

"Local Government Response to Bioterrorist Attacks." Public Entity Risk Institute (PERI).
http://www.riskinstitute.org/lib_art.asp?art_id=1025. [2002-OCT-25]
Extensive list of resources and critical information on how to prepare your city or town.

"NACCHO Responds to Bioterrorism." NACCHO.
http://www.naccho.org/files/documents/responds_to_bioterrorism.html. [2002-OCT-25]
Links to information on bioterrorism awareness and prevention geared towards local health officials.

"Top 10 Suggestions from State Health Officials Who've Been There." National Governors Association. http://www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_3053,00.html. [2002-OCT-25] Straightforward suggestions on what steps local health officials should take to prepare for a bioterrorism incident.

"Tulsa Gears Up for Bioterrorism." National Journal. 14 Sept 02, pp. 2613-14.
Local Example of bioterrorism preparedness.

"Public Health Emergency Preparedness and Response." Center for Disease Control and Prevention. http://www.bt.cdc.gov/. [2002-OCT-25]
Portal site for bioterrorism.

"Chemical and Biological Terrorism." Public Entity Risk Institute.
http://www.riskinstitute.org/lib_art.asp?art_id=1015. [2002-OCT-25]
Describes types of chemical and biological agents, lists examples of local public health initiatives and contains a large list of resources to go to for more help.

"Terrorism and Emergency Preparedness: Local Government Bio Terror Links". *Public Technology, Inc*. http://pti.nw.dc.us/task_forces/emergency_management/index.html. [2002-OCT-25] Contains many local bioterror links, provides case examples from municipal government websites.

"Smallpox Response Plan and Guidelines." CDC.
http://www.bt.cdc.gov/agent/smallpox/response-plan/index.asp. [2002-OCT-25]
Comprehensive prevention and response guidelines for local health officials and experts.

"Advisories on Anthrax, Mail, and Related Topics." Chemical and Biological Defense Information Analysis Center.
http://www.cbiac.apgea.army.mil/resources/directory/anthrax_info.htm. [2002-OCT-25]
Numerous resources for a wide range of topics related to biological and chemical terrorism.

Center for Civilian Biodefense Strategies. http://www.hopkins-biodefense.org/ [2002-OCT-25]

"Countering Bioterrorism and Other Threats to the Food Supply." Foodsafety.gov.
http://www.foodsafety.gov/~fsg/bioterr.html. [2002-OCT-25]
Portal site to federal resources regarding food safety (Agroterrorism).

"Frequently Asked Questions about Food Safety and Terrorism." U.S. Food and Drug Administration. http://www.cfsan.fda.gov/~dms/fsterrqa.html. [2002-OCT-25]

"Responding First to Bioterrorism." The National Academies. http://www.nap.edu/shelves/first/. [2002-OCT-25] Portal site for first-responder resources regarding bioterrorism.

"21st Century Guide to Bioterrorism, Biological and Chemical Weapons, Germs and Germ Warfare, Nuclear and Radiation Terrorism." Naval Operational Medical Institute.
http://forum.nomi.med.navy.mil/cd/CD085/09%20p2%20NBC%20TERRORISM%20GUIDE/contents.PDF. [2002-OCT-25]

List of terrorism links from a government standpoint. Includes reports, and information on training, prevention, and identifying the threat.

"Advice for Securing Buildings against a chemical or biological attack." Lawrence Berkeley National Laboratory. http://securebuildings.lbl.gov/. [2002-OCT-25]
Prevention advice and training tips.

"Biological and Chemical Weapons." National Institute of Health: MEDLine Plus. http://www.nlm.nih.gov/medlineplus/biologicalandchemicalweapons.html. [2002-OCT-25]
Contains a wide range of health related information.

"Chemical Agent Lists and Information." CDC. http://www.bt.cdc.gov/Agent/agentlistchem.asp. [2002-OCT-25] List of chemical agents commonly found in weapons, links to critical info, emergency procedures.

"Chemical Emergency." FEMA. http://www.fema.gov/pdf/rrr/talkdiz/chemical.pdf. [2002-OCT-25] Guidebook for emergency management in case of a major chemical emergency.

"Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks." May 2002. CDC: National Institute for Occupational Safety and Health. http://www.cdc.gov/niosh/bldvent/pdfs/2002-139.pdf. [2002-OCT-25]
Specific recommendations on how to protect indoor environments from airborne chemical/biological/radiological agents.

"LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan." EPA – Chemical Emergency Preparedness and Prevention Office (CEPPO). August 2001. http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/lepcct.pdf/$file/lepcct.pdf [2002-OCT-25]
Information for local governments regarding procedure after a deliberate chemical release.

"Managing Hazardous Materials Incidents." CDC. Agency for Toxic Substances and Disease Registry. http://www.atsdr.cdc.gov/mhmi.html. [2002-OCT-25]
A planning guide to help first responders respond to hazardous materials incidents.

"Other Terrorism." Center for the study of Bioterrorism, Saint Louis University. http://www.slu.edu/colleges/sph/csbei/bioterrorism/other.htm [2002-OCT-25]
Information on chemical and biological weapons.

"ToxFAQ's– Frequently Asked Questions about Contaminants Found at Hazardous Waste Sites." Agency for Toxic Substances and Disease Registry. http://www.atsdr.cdc.gov/toxfaq.html. [2002-OCT-25]
List of hazardous chemicals and their effects.

"Weapons of Mass Destruction Training Program." Department of Justice – Office of Domestic Preparedness." http://www.ojp.usdoj.gov/odp/docs/coursecatalog.pdf. [2002-OCT-25]
Course catalog for all Department of Justice Training Programs, including chemical, biological, and other mass-destruction attacks.

3. Nuclear and Radiological Attacks

It is the ultimate nightmare scenario for local officials—and, indeed, for all Americans. A terrorist-launched nuclear or radiological attack on an American city could cause large numbers of casualties while provoking widespread panic and disruption.

At Issue

Radiological or Nuclear: Defining the Difference. A nuclear weapon is any weapon that uses a nuclear reaction (fission of an atom or fusion of two atoms) for its explosive power. Nuclear weapons include missiles, bombs, artillery rounds, and mines.

Radiological weapons, by contrast, are weapons that simply use radiological material to cause panic and loss of life. According to the Carnegie Endowment for International Peace, the spectrum of radiological attacks ranges from low-level nuclear waste planted as a package in an urban location, through highly toxic nuclear material exploded as a "dirty bomb," using conventional explosives to spread it over a wide area.

Assessing the Threat. According to the experts, terrorists could conceivably launch a nuclear or radiological attack on domestic targets in the United States in one of three ways:

> **"Loose nukes."** According to the Council on Foreign Relations, the term "loose nukes" originally referred to poorly guarded nuclear weapons in the former Soviet Union that might tempt terrorists or criminals. Today, experts use the term to refer to nuclear weapons, materials, or know-how that could fall into the wrong hands. The International Atomic Energy Agency (IAEA) has reported 175 nuclear smuggling incidents since 1993, 18 of which involved highly enriched uranium, the key ingredient in an atomic bomb and the most dangerous product on the nuclear black market. For more information: www.terrorismanswers.com/weapons/loosenukes.html
>
> **"Dirty bombs."** A dirty bomb--also known as a radiological dispersion bomb--is a relatively unsophisticated device that combines radioactive materials with conventional explosives. When exploded, such a device scatters radioactive particles into the environment. While the number of casualties involved in a dirty bomb explosion would likely be minimal when compared to the detonation of a nuclear weapon, a dirty bomb is appealing to terrorists because of its ability to cause panic and disruption. As an alternative to exploding a dirty bomb, terrorists could cause a similar panic simply by placing low-level radioactive waste at a location in the community. For more information: www.terrorismanswers.com/weapons/dirtybomb2.html
>
> **Direct attack on a nuclear facility.** In a paper prepared for a recent meeting of the International Atomic Energy Agency, nuclear terrorism expert Gavin Cameron called reactors "potentially attractive targets for terrorists." The reason: they offer a means for a terrorist group to achieve a spectacular attack that sets them apart from other groups and ensures that they are noticed as an organization. Pointing out that the September 11th attackers apparently considered targeting U.S. nuclear facilities, Cameron observed that such an attack is no longer a far-fetched notion. More likely than an air attack, however,

would be a truck bomb attack. Whether such an attack could lead to the release of radiological material is uncertain. For more information: http://www.iaea.or.at/worldatom/Press/Focus/Nuclear_Terrorism/cameron.pdf

The Impact of a Radiological Attack

"A radiological attack would most likely involve lower-level radioactive material or even nuclear waste. Depending on what the material was and the amount of conventional explosive that was used to spread it around, it would potentially sicken people and contaminate large swaths of territory. However, it would not kill thousands of people outright, as would a nuclear explosive blast. But even a small amount of radioactive material, if planted in an urban setting, would have the potential to sow considerable panic unless authorities were quickly able to neutralize the incident in the public's mind."

From testimony of Rose Gottemoeller, Senior Associate of the Carnegie Endowment for International Peace, before a House subcommittee in September 2002. For the complete text: http://www.ceip.org/files/Publications/Nuclearandradiologicalterrorism.asp

Ideas for Local Action

Preventing a Dirty Bomb Attack. Of the three scenarios outlined above for a radiological attack by terrorists on a U.S. domestic target, the most likely, according to experts, would be the explosion of a dirty bomb.

The primary means of preventing a dirty bomb attack in the United States centers on intelligence gathering about possible strikes, as well as the use of radiation-detection equipment to monitor suspicious cargo at borders.

Nevertheless, localities can play an important role as well. In Times Square during New Year's Eve 2001, for example, the New York Police Department used Geiger counters to detect potential dirty bombs; radiation detectors were also later installed outside some city-owned buildings in New York.

Responding to a Radiological Attack. According to the Council on Foreign Relations, the Federal Emergency Radiological Response Plan, drawn up in 1996 and rehearsed regularly, covers many scenarios related to the release of radiation. The Federal Emergency Management Agency (FEMA) would coordinate the response by several civilian and military entities. After dealing with the initial blast, the top priorities would be the treatment of radiation sickness, the containment and monitoring of radioactive fallout, evacuation, and decontamination.

The local response, of course, would center on managing casualties and providing information to the public. The following guidelines for first responders come from the CDC Factsheet, "Casualty Management After a Deliberate Release of Radioactive Material" (www.cdc.gov/nceh/radiation/casualties_radioactive.htm)

- Seriously injured people should be removed from the source of radiation, stabilized, and sent to hospitals first.
- After treatment of serious physical injuries, preventing the spread of the radioactive material or unnecessary exposure of other people is paramount. Carry out the following immediate response actions without waiting for any radiation measurements.
    - Establish an exclusion zone around the source. Mark the area with ropes or tapes. Reroute traffic. Limit entry to rescue personnel only. Detain uninjured people who were near the event or who are inside the control zone until they can be checked for radioactive contamination, but do not delay treatment of injured people or transport to a hospital for this purpose.
    - Take action to limit or stop the release of more radioactive material, if possible, but delay cleanup attempts until radiation protection technicians are on the scene.
    - Tell nearby hospitals to expect the arrival of radioactively contaminated and injured people.
- Everyone near the scene should be checked for radioactive contamination. As soon as you can obtain radiation measuring equipment, establish a decontamination area for this purpose. Decontaminate people whose injuries are not life-threatening (broken arms, etc.) before sending them to hospitals. Do not send people without physical injuries to hospitals.
- Record-keeping is as important for the long-term health of the victims as it is for the emergency responders. CDC has developed a form that allows first responders to record contact information for all exposed people so they can be given medical examinations later. The Department of Health and Human Services will request this information later.

In the event of a radiation emergency, CDC advises localities to notify the state Radiation Control Program Director. Telephone numbers for each state may be found at http://www.crcpd.org/Map/map.asp

Resources

"Dirty Bombs." Council on Foreign Relations. 'Terrorism: Questions and Answers.' http://www.terrorismanswers.com/weapons/dirtybomb2.html. [2002-OCT-30]
Basic information about dirty bombs.

"Loose Nukes." Council on Foreign Relations. 'Terrorism: Questions and Answers.' http://www.terrorismanswers.com/weapons/loosenukes.html. [2002-OCT-30]
Basic information about loose nuclear weapons.

"Nuclear Terrorism: Reactors and Radiological Attacks after September 11." International Atomic Energy Agency.
http://www.iaea.or.at/worldatom/Press/Focus/Nuclear_Terrorism/cameron.pdf. [2002-OCT-30]
Describes in detail the threat of terrorist attacks to nuclear reactors, especially from insiders in a country.

"Nuclear and Radiological Terrorism." Carnegie Endowment for International Peace – Proliferation Brief, 5:14 [2002-OCT-01]
http://www.ceip.org/files/projects/npp/pdf/Testimony/RoseGsept242002.pdf.
Testimony before Congress on Sept. 24, 2002 regarding radiological terrorism.

"Pascal's New Wager: The Dirty Bomb Threat." Center for Defense Information (CDI).
http://www.cdi.org/terrorism/dirty-bomb.cfm. [2002-OCT-01]
Information on dirty bombs.

"Radiation Studies – Emergency Response." CDC. National Center for Environmental Health.
http://www.cdc.gov/nceh/radiation/response.htm. [2002-OCT-01]
Links to emergency response fact sheets, info about various types of radiation emergencies including nuclear attacks and dirty bombs.

"Some See Panic as Main Effect of Dirty Bombs." New York Times (March 7, 2002)
http://www.nytimes.com/2002/03/07/politics/07NUKE.html. [2002-OCT-01]
Information on dirty bombs.

"State Radiation Control Agencies." Conference of Radiation Control Program Directors, Inc.
http://www.crcpd.org/map/map.asp. [2002-OCT-01]
Lists state-by-state radiation control contacts.

4. Cyberterrorism

It may not strike the same fear in people as the notion of a radiological, chemical, or biological attack, but cyberterrorism can pose a very real threat to American communities.

At Issue

Cyberterrorism Defined. In recent testimony before a U.S. House of Representatives panel, Dorothy E. Denning of Georgetown University's Institute for Information Assurance defined cyberterrorism as "the use of information technology by terrorist groups and individuals to further their agenda." What distinguishes cyberterrorism from the work of every-day cyberthieves and thrill-seeking computer hackers, according to Denning, is the potential of cyberterrorism to inflict grave harm and loss of life. (See her full testimony at www.cs.georgetown.edu/~denning/infosec/cyberterror.html)

The Council on Foreign Relations (CFR) expands on this definition in a Q&A fact sheet on its website (http://www.terrorismanswers.com/terrorism/cyberterrorism.html):

> "Like other terrorist acts, cyberterror attacks are typically premeditated, politically motivated, perpetrated by small groups rather than governments, and designed to call attention to a cause, spread fear, or otherwise influence the public and decision-makers."

Terrorists, according to the CFR, try to leverage limited resources to instill fear and shape public opinion, and dramatic attacks on computer networks could provide a means to do this with only small teams and minimal funds. Moreover, "virtual" attacks over the Internet or other networks allow attackers to inflict terror from far away, making borders, X-ray machines, and other physical barriers irrelevant.

Terrorists might also try to use cyberattacks to amplify the effect of other attacks. For example, they might try to block emergency communications or cut off electricity or water in the wake of a conventional bombing or a biological, chemical, or radiation attack. Many experts, according to CFR, say that this kind of coordinated attack might be the most effective use of cyberterrorism.

Types of Cyberterror Attacks. Regardless of their political or operational objectives, terror attacks launched in cyberspace would be designed to exploit vulnerabilities in computer security: computer viruses, stolen passwords, insider collusion, software with secret "back doors" that intruders can penetrate undetected, and orchestrated torrents of electronic traffic that overwhelm computers—also known as "denial of service" attacks.

Attacks also could involve stealing classified files, altering the content of Web pages, disseminating false information, sabotaging operations, erasing data, or threatening to divulge confidential information or system weaknesses unless a payment or political concession is made.

What Could Cyberterrorists Do?

Although experts debate the capacity of terrorists to employ information technology alone to cause severe harm to people and infrastructure, attacks could conceivably accomplish the following:

- Overload telephone lines with special software;
- Disrupt the operations of air traffic control as well as shipping and railroad computers;
- Scramble the software used by major financial institutions, hospitals, and other emergency services;
- Alter by remote control the formulas for medication at pharmaceutical plants;
- Change the pressure in gas pipelines to cause a valve failure; or
- Sabotage the New York Stock Exchange.

Source: "Cyberterrorism…Cybercrime…Cyberwarfare." Center for Strategic and International Studies (http://www.csis.org/pubs/cyberfor.html).

The Likelihood of Attack. According to Denning, cyberterrorism, while a "real possibility," poses significant challenges to terrorists. Citing an August 1999 report from the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California, Denning pointed out that "the barrier to entry for anything beyond annoying hacks is quite high and … terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation."

Nevertheless, Denning and others caution officials at all levels of government to prepare for the worst. "At least for now, hijacked vehicles, truck bombs, and biological weapons seem to pose a greater threat than cyber terrorism," she observed in a November 2001 article for the Social Science Research Council. "However, just as the events of September 11 caught us by surprise, so could a major cyber assault. We cannot afford to shrug off the threat." (See the article at http://www.ssrc.org/sept11/essays/denning.htm.)

Ideas for Local Action

Beefing Up Computer Security. The most obvious way to prevent cyberterrorism from posing a threat to American communities is for public and private sector officials to become more vigilant about computer security. According to the Council on Foreign Relations, that means patching security flaws quickly once they're detected, designing systems to withstand attacks, backing up systems off-site so they can bounce back quickly from a disruption, and watching for disgruntled employees who might help terrorists penetrate a system.

Recommendations for Local and State Officials. In October 2001, President Bush signed an executive order establishing the President's Critical Infrastructure Protection Board (CIPB). In its *National Strategy to Secure Cyberspace* issued less than one year later, the board made a series of recommendations for action by all levels of government, as well as the private and nonprofit sectors. The three recommendations for state and local governments were:

1. State and local governments should consider establishing information technology (IT) security programs for their departments and agencies, including awareness, audits, and standards. State, county, and city associations should consider providing assistance, materials, and model programs.

2. State and local governments should consider participating in the information sharing and analysis centers (ISACs) established as part of the federal government's infrastructure protection planning. (For a directory of ISACs that have been established to date, see www.nipc.gov/infosharing/infosharing6.htm)

3. State and local governments should consider expanding training programs in computer crime for law enforcement officials, including judges, prosecutors, and police. The Federal government could assist in coordinating such training and explore whether funding assistance is feasible.

For the full draft of the *National Strategy to Secure Cyberspace*, see http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html.

Protecting Your Local Government Systems. In an article prepared for the November 2001 symposium, "Community Response to the Threat of Terrorism," attorney Robert Thetford offered a number of very specific steps for local governments and businesses to take to protect themselves from cyberterror. These include:

Policy review. Thetford, who co-founded the Institute for Criminal Justice Education, Inc., recommends an immediate review of current practices and procedures connected to the use of information technology based on such questions as:

- Who has access and to which systems?
- What is their level of access?
- Exactly what are employees able to do with their access?
- Are written policies in place?
- Are they enforced?

Policy reviews, according to Thetford, should address e-mail and Internet use as well as basic security practices. He also urges local governments and businesses to consider using an on-system warning screen to advise users that the system confers no privacy rights and is to be used by authorized personnel only for official government business. The warning should further advise that system resources are subject to being retained and reviewed by the government and may be furnished to others, including law enforcement agencies, at the discretion of the government.

Firewalls and Virus Checkers. Computers and networks without operating firewalls and up-to-date virus protection, according to Thetford, are similar to open entrance doors in homes; they are invitations for criminals to enter, steal, and vandalize.

Firewalls are generally considered necessary when using "always-on" connections like T1 lines, cable, and DSL connections because a typical telephone modem for a home line uses a different computer address (URL) each time the server is dialed. Virus checkers, on the other hand, are relatively cheap and offer substantial protection from e-mail and Web viruses, but must be frequently updated to be effective.

Because no virus checking software offers 100 percent protection, Thetford recommends limiting Internet access only to those employees who have a need for Internet use in their jobs. He adds that e-mail use also should be examined and policies formulated to restrict the receipt of attachments, which often contain viruses.

Security Patch Updates. Thetford says that many attacks on computer systems could be thwarted simply by installing system patches provided by software manufacturers to plug known security breaches. Network administrators and individuals should check system vendor sites on a regular basis for upgrades designed to repair system deficiencies.

Along the same lines, administrators should frequently check the FBI's National Infrastructure Protection Center (www.nipc.gov) and Carnegie Mellon University's federally funded CERT Coordination Center (www.cert.org), for updated cyberattack information. The National Infrastructure Protection Center (NIPC) also provides a forum (InfraGard) that encourages the exchange of information about cyberterror and related threats between the public and private sectors. InfraGard may be accessed through the NIPC site above or directly through www.infragard.net.

Data Backup. One of most common complaints among computer users involves system crashes, whether they are caused by a virus, sabotage, or malfunction. Other than virus protection, the easiest and cheapest way to protect a system is through periodic data backups, says Thetford. Most home users and small businesses seldom backup their data on a frequently scheduled basis, and when the crash comes, which it inevitably does, weeks or months of work can be lost. Nor is it enough to simply copy the data. Provisions should be made to store the data at a secure off-site location for fire and theft protection.

Thetford recommends that backup procedures and schedules be thoroughly covered in the governmental policy or procedure manual. In addition to electronic data backup, vital hard copy files should also be archived for the unlikely event that extended power or computer outages might occur. Protection against transient power outages should be provided by UPS battery backup systems to eliminate unnecessary down time, with thought given to implementing generator-supplied power supply for the entire computer system.

Internal Security. Finally, because most of the computer attacks today, including vandalism and theft, still originate from within organizations, governments and businesses need to give more consideration to internal security. Information technology

training, security education, and employee screening are all tools used to safeguard against internal attacks and theft.

Periodic security audits from trusted outside agencies offer an unbiased view of the level of protection offered, as well as providing notice to employees that infractions will likely be discovered and appropriate sanctions imposed.

For more information: http://www.riskinstitute.org/lib_art.asp?art_id=1014

What Are the Laws in Your State?

At the same time that many local governments are working to respond to the cyberterror threat, state lawmakers have been struggling with many of the same issues. The following information about state actions on this issue comes from the National Conference of State Legislatures:

- At least ten states have pending legislation that addresses cyberterrorism;
- At least three states--California, Georgia, and Pennsylvania--have laws specifically aimed at electronic terroristic threats or acts;
- Nearly every state has statutes banning hacking and unauthorized access; and
- At least sixteen states ban unleashing harmful computer viruses and contaminants.

For more information, see http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm

Resources

"Is Cyber Terror Next?" by Dorothy E. Denning, Professor of Computer Science; Director of the Georgetown Institute for Information Assurance, Georgetown University. Social Science Research Council. http://www.ssrc.org/sept11/essays/denning.htm. [2002-NOV-01]
Discusses possibility of a cyberterror attack on the United States.

"National Strategy to Secure Cyberspace." The President's Critical Infrastructure Protection Board. http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html. [2002-NOV-01]
A draft report on the topic from a presidentially appointed panel.

"Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." http://www.nautilus.org/info-policy/workshop/papers/denning.html. [2002-NOV-01]
Historical examples of cyberterrorism and hacking for foreign policy intelligence, and an outline of the threat today.

Critical Infrastructure Assurance Office. http://www.ciao.gov/. [2002-NOV-01]
Federal Government agency in charge of internet security.

"Cyberterrorism." National Conference of State Legislatures.
http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm. [2002-NOV-01]
Portal site including description of threat, current policy, and resources.

"Cyberterrorism: Fact or Fancy?" FBI Laboratory.
http://www.cs.georgetown.edu/~denning/infosec/pollitt.html. [2002-NOV-01]
This paper discusses the definition of cyberterrorism, its potential, and suggests an approach to the minimization of its' dangers.

"Cyberterrorism…Cybercrime…Cyberwarfare." Center for Strategic and International Studies.
http://www.csis.org/pubs/cyberfor.html. [2002-NOV-01]
Description and history of cyberterrorism, and recommendations.

"Cyberterrorism and Government Warfare: Government Perspectives." By Michael Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation. http://www.terrorismcentral.com/Library/Teasers/vatis.html. [2002-NOV-01]
Defines the threat of cyberterrorism from the perspective of the FBI.

"Cyberterrorism drill set - Operation Dark Screen to help government, industry prepare for attacks" Federal Computer Week (July 22, 2002).
http://www.globalsecurity.org/org/news/2002/020722-fcw1.htm. [2002-NOV-01]
Information to help people in many arenas better understand their roles in preparing for, recovering from, and protecting the nation's critical infrastructure during a cyberattack.

"Cyberterrorism Resource Center." Global Development Center.
http://www.globaldisaster.org/cyberterrorrescen.shtml. [2002-NOV-01]
Up-to-date news on "cyber-warfare", also has cyberterrorism resources.

"Defending America Against Cyberterrorism." ZDNet News. http://zdnet.com.com/2100-1105-531071.html. [2002-NOV-01]
Interview with Richard Clark, adviser to the President for cybersecurity.

"Electronic Crime Publications." National Institute of Justice.
http://www.ojp.usdoj.gov/nij/sciencetech/ecrime_pub.htm. [2002-NOV-01]
List of electronic prime publications, and a searchable abstracts database.

"Electronic Threats and Terroristic Activities." National Conference of State Legislatures.
http://www.ncsl.org/programs/lis/CIP/electerthreat.htm.
Several states have addressed terrorism in state criminal codes, including statutes that address terroristic activities and threats.

"FBI Briefs Homeland Task Force on Cyberterrorism." National Association of Counties.
http://www.naco.org/pubs/cnews/01-12-10/fbi.htm. [2002-NOV-01]
The role of technology in assisting counties to secure America was the theme for the second meeting of the National Association of Counties' Homeland Security Task Force, which gathered Nov. 28 in Santa Fe County, N. M.

"GAO Testimony on Critical Infrastructure Protection." Robert F. Dacey, Director, Information Security Issues, General Accounting Office. [2002-NOV-01]
http://www.terrorismcentral.com/Library/Teasers/GAO.html.
Review/oversight hearing for the National Infrastructure Protection Center (NIPC).

"Government Info Sharing Key To Fighting Terrorism." CIO.com.
http://www.cio.com/government/edit/122001_share.html. [2002-NOV-01]
U.S. government officials spoke at a crisis management conference Dec. 18 (2001).

"Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism." Jan. 1999. National Institute of Justice. http://www.ncjrs.org/pdffiles1/173384.pdf. [2002-NOV-01]
An inventory of State and local law enforcement agencies that is being used to determine the technologies needed by these agencies to combat terrorism.

National Infrastructure Protection Center. http://www.nipc.gov/. [2002-NOV-01]
The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.

"New York Enlists Private Sector in Fight Against Cyberterrorism." Washington Technology.
http://www.washingtontechnology.com/news/1_1/daily_news/17961-1.html. [2002-NOV-01]
Information on how the state of New York protects its information systems and critical infrastructure against terrorist attacks.

"Terrorism: Questions and Answers – Cyberterrorism" Council on Foreign Relations.
http://www.terrorismanswers.com/terrorism/cyberterrorism.html. [2002-NOV-01]
Frequently asked questions about cyberterrorism.

"Testimony before the Special Oversight Panel on Terrorism." Denning, Dorothy.
http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. [2002-NOV-01]
Testimony of Dening, a Georgetown University Professor/Cyberterrorism expert, before a special congressional committee.

"The Challenge of Cyberterrorism." Public Entity Risk Institute.
http://www.riskinstitute.org/lib_art.asp?art_id=1014. [2002-NOV-01]
Article about attack methods, potential targets, the future, and preparedness.

"The Cyberterrorism Czar – What's Next?" Robert Lemos, CNET.com news.
http://news.com.com/2102-1082-275751.html. [2002-NOV-01]
Article about Richard Clark, Adviser to the President for Cybersecurity.

"The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge." Institute for Security and Intelligence. http://afgen.com/terrorism1.html. [2002-NOV-01]
Insight into cyberterrorists' actions and goals.

U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section. http://www.cybercrime.gov/. [2002-NOV-01]
Investigative wing of the Dept. of Justice on computer crime.

"What is Cyber-terrorism?" SANS Institute. http://rr.sans.org/infowar/cyberterrorism.php. [2002-NOV-01]Overview of the cyberterrorism threat with an extensive list of resources and web links.

5. Interoperability

Responding to a terror incident requires effective coordination, communication, and sharing of information among numerous criminal justice and public safety agencies. Improving the interoperability of public safety communications is one of the most critical steps local governments can take to ensure an effective response.

At Issue

Interoperability Defined. Interoperability is "the ability of public safety personnel to communicate by radio with staff from other agencies, on demand and in real time." This is the definition developed by the Public Safety Wireless Network (PSWN) Program, a federal government initiative launched in the 1990s to promote "seamless, coordinated, and integrated public safety communications." In addition to radio communications, interoperability is often used to refer to computer links and other means of coordinating public safety operations across jurisdictions and levels of government.

Three Types of Interoperability. Public safety agencies generally require three distinct types of interoperability:

- *Day-to-day interoperability* involves coordination during routine public safety operations. Interoperability is required, for example, when firefighters from around a county join forces to battle a structural fire or when neighboring law enforcement agencies must work together during a vehicular chase.

- *Mutual aid interoperability* involves a joint and immediate response to catastrophic accidents or natural disasters and requires tactical communications among numerous groups of public safety personnel. Airplane crashes, forest fires, earthquakes, and hurricanes are examples of mutual aid events.

- *Task force interoperability* involves local, state, and federal agencies coming together for an extended period of time to address a public safety problem. Task forces lead the extended recovery operations for major disasters, provide security for major events, and conduct operations in response to prolonged criminal activity.

For more information, see "Public Safety and Wireless Communications Interoperability," a PSWN fact sheet at www.pswn.gov/library/docs/interop_guide.doc.

Documenting Interoperability Problems. Interoperability is critical to the ability of the public safety community to provide a coordinated response to terrorist activities and other threats. Analysis of events ranging from the 1995 Oklahoma City bombing to the shootings at Colorado's Columbine High School in 1989 to the terrorist attacks on September 11, 2001, all point to interagency communications as one of the weakest links in emergency management. The key problem: existing systems do not enable communication across agencies or levels of government.

Two PSWN surveys in 1998 asked more than 2,000 law enforcement, fire, and emergency medical service agencies to reflect on the major obstacles to interoperability. Among those cited: spectrum and funding limitations, as well as incompatible technologies and the lack of adequate systems planning.

- *Spectrum Limitations.* Public safety radio spectrum refers to the array of channels, like those on a television, available for communications transmissions. Scarce spectrum results in congested radio channels and increased interference, limiting the ability of public safety personnel to communicate. Additional spectrum is needed to meet current communication needs and to support the deployment of new technologies. A related problem is the fragmentation of spectrum—i.e., current public safety channels are located in several portions of the radio spectrum, resulting in separate spectrum "islands" that isolate public safety operations and jurisdictions.

- *Funding Limitations.* Many existing public safety communications systems cannot support modern technologies that are needed for interoperability. Replacement of outdated systems or system expansions is expensive. Inadequate funding for upgrades often prevents a public safety agency from purchasing the technology and equipment that can enhance interoperability and improve organizational effectiveness

- *Incompatible Technologies.* A variety of new radio technologies are becoming increasingly popular as agencies plan to replace or upgrade their existing systems. Despite these new technologies, competing equipment vendors continue to manufacture, and public safety agencies continue to purchase, equipment that is not interoperable. Radio communications equipment produced by multiple vendors uses proprietary and incompatible technology schemes. These incompatibilities prevent interoperability even when the radios operate in the same spectrum bands.

- *Lack of Systems Planning.* A lack of adequate planning during systems development can preclude interoperability. A broad range of complex architectural, operational, and organizational issues must be addressed in planning system upgrades, including coordinating and sharing resources to develop joint communications systems, developing operational requirements for coordinated emergency responses, and implementing system security measures.

Ideas for Local Action

Advocate for Federal Action. Recognizing that reliable and interoperable wireless communications are essential to public safety, the National League of Cities and others have called on the federal government to take immediate steps to provide local governments with the funding and the broadcast channels needed to enhance their emergency communications capabilities.

Along with the International Association of Chiefs of Police, the National Association of Counties, and other organizations, NLC has urged Congress and the FCC to implement a comprehensive plan that meets requirements for sufficient spectrum allocation, as well as 9-1-1 services, technology deployment and procurement, and long-term contingency planning.

Of the $37.7 billion the Bush Administration proposed for homeland security in its fiscal year 2003 budget request to Congress, about $3.5 billion would go to communities for equipment and training for first responders, including $1.6 billion for equipment for interoperable communications systems and other networks.

According to a June 2002 article in *Nation's Cities Weekly*, Representative Curt Weldon (R-Pa.), chairman of the House Armed Services Committee's military procurement subcommittee, said more of the technologies developed for military purposes should be transferred for civilian use to help public safety agencies respond to emergencies. The congressman also noted that he and other lawmakers were pushing legislation that would free up 24 MHz of spectrum allocated for public safety purposes in the 700 MHz band.

The Homeland Emergency Response Operations Act (H.R. 3397) would set a firm deadline of December 31, 2006, by which the federal government must give public safety agencies the broadcast frequencies Congress set aside for them as part of the Balanced Budget Act of 1997. Congress agreed to let broadcasters keep this portion of spectrum until 85 percent of the television sets in their markets were capable of receiving digital signals.

In other advocacy on interoperability issues, NLC and others are calling on the federal government to encourage regional planning for public safety communication needs. NLC's policies on public safety communications are detailed further in two chapters of the National Municipal Policy: Public Safety and Crime Prevention; and Information Technology and Communications. See http://www.nlc.org/nlc_org/site/policy_legislation/policy/national_municipal_policy.cfm

Contact State Officials. When the FCC designated approximately 10 percent (2.6 MHz) of the 700 MHz public safety spectrum for nationwide interoperable communications, the agency determined that administration of the interoperability channels should occur at the state level, either through a newly established State Interoperability Executive Committee (SIEC) or an existing agency.

The first responsibility of the state entity charged with this task is to develop an interoperability plan. The agency also is charged with deciding who will hold the license for the interoperability spectrum as well as resolve licensing issues. Other responsibilities involved in administering the interoperability channels include the creation and oversight of incident response protocols, creation of chains of command for incident response and reporting, and executing Memoranda of Understanding and Sharing Agreements. Each state was required to notify the FCC by December 31, 2001 of its decision. For information about what is happening in your state, as well as state-level contacts, see http://wireless.fcc.gov/publicsafety/700MHz/interop-contacts.html

Develop Local Solutions: Lessons from the Pentagon Attack. A PSWN report, *Answering the Call: Communications Lessons Learned from the Pentagon Attack*, provides a detailed analysis of public safety communications following the terrorist attack on the Pentagon on September 11, 2001. The report also includes steps public safety agencies across the country can take to improve their radio communications.

A total of 50 public safety agencies responded to the Pentagon attack, resulting in approximately 900 radio users attempting communications. After interviewing first responders, technical representatives, and public information officers from the public safety agencies involved, PSWN came to the following conclusions:

- *Regional Planning and Coordination Effort.* Because of the unique geographical and political environment of the Washington, D.C., metropolitan area, its public safety leaders realized many years ago that any response to a major incident in the area would be a regional response. With the Metropolitan Council of Governments (COG) providing a proactive forum for planning and coordination, local jurisdictions instituted plans and procedures for mutual-aid interoperability. These plans are used on a daily basis by most local agencies, greatly reducing confusion for responding agencies.

- *Training.* Washington, D.C. metropolitan area agencies regularly conduct mass casualty and incident drills that bring together the various local agencies to effect a large-scale response. Through these drills, agencies rehearse the necessary operational and communications procedures. Additionally, interoperability training occurs on a day-to-day basis when public safety workers respond to routine incidents in other jurisdictions.

- *Incident Command System.* The early establishment and strict adherence to a formal Incident Command System (ICS) was a key factor supporting successful communications at the Pentagon attack. The ICS was flexible and scalable, and allowed the Incident Commander to track and oversee all facets of the operations.

- *Commercial Services Usage.* Major incidents, regardless of location, have shown that commercial service networks are not designed to handle the immense volume of calls generated at or near an incident scene. Responders found that the only reliable form of communications were their own private land mobile radio systems.

- *Lack of Interoperability Among State and Federal Responders.* During the initial response, the majority of local public safety responders experienced no difficulty establishing interoperable communications on the scene. This was because of the high level of regional coordination and previously established agreements. However, as the number of state and federal agencies (secondary responders) increased at the site, interoperability presented new challenges. No means of direct interoperability was immediately available to these secondary response agencies.

- *Interoperability Assets Inventory.* An inventory list of interoperability assets (i.e., mobile command vehicles, switches, and extra radios) available in the Washington, D.C. metropolitan region does not exist.

- *"Total Interoperability" Requirement.* First responders require seamless communications. However, the level of interoperability necessary to support operations for secondary, or support responders, has not been documented.

For more information, see http://www.pswn.gov/library/pentagon_release_2_1.htm

Enhancing Interoperability in Your City or Town

Based in part on its analysis of the public safety response to the September 11, 2001, Pentagon attack, the PSWN Program developed the following recommendations for agencies to enhance communications interoperability in responding to routine and major incidents:

- Develop regional and statewide communications systems that can support interoperable communications among multiple agencies.
- Establish mutual-aid agreements and standard operating procedures--not only among local agencies, but also with state and federal public safety agencies.
- Employ the Incident Command System (ICS) to enhance communications efforts in emergency response situations.
- Conduct mass casualty and disaster response training drills to identify existing capabilities and potential shortfalls.
- Conduct a communications asset inventory to identify tools and their capabilities.
- Adhere to common technology standards in the design, procurement, and implementation of future public safety communications systems.

For more information, see http://www.pswn.gov/library/pentagon_release_2_1.htm

Resources

"Community Demonstration Project." Federal Geographic Data Committee. http://www.fgdc.gov/nsdi/docs/cdp.html. [2002-OCT-30]
Government pilot project that hopes to show how GIS mapping can solve community problems.

"Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study. MIPT. http://www.mipt.org/cbacifindings.asp. [2002-OCT-30]
Discusses chain of command during Oklahoma City Bombing.

"FCC Clears the Air for Safety." Federal Communication Weekly. (June 24, 2002). http://www.fcw.com/supplements/homeland/2002/sup2/hom-wire1-06-24-02.asp. [2002-OCT-30] News article about FCC's new 700MHz initiative.

"Homeland Security and Geographic Information Systems." Federal Geographic Data Committee. http://www.fgdc.gov/publications/homeland.html. [2002-OCT-30]
Information on GIS systems.

"Homeland Security Outlook." American City and County (1 Aug 2002). http://www.americancityandcounty.com/ar/government_homeland_security_outlook/index.htm. [2002-OCT-30] Examining local government cooperative agreements and needs for hometown security.

"Interoperability Spectrum." Federal Communications Commission (FCC). http://wireless.fcc.gov/publicsafety/700MHz/interop.html. [2002-OCT-30]
Current proceedings, news, FAQ for 700MHz radio frequency for emergency responders.

"Interoperability Spectrum Contacts." FCC. http://wireless.fcc.gov/publicsafety/700MHz/interop-contacts.html. [2002-OCT-30]
State contact info regarding 700MHz radio frequency interoperability.

"Oklahoma City – Seven Years Later: Lessons for Other Communities. Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT). http://www.mipt.org/pdf/MIPT-OKC7YearsLater.pdf [2002-OCT-30]

"Partners in Progress." Fire Chief. August 2002. http://firechief.com/ar/firefighting_partners_progress/index.htm. [2002-OCT-30]
Six city managers discuss their relationship with the fire department.

"Preparing for Terrorism: What Every Manager Needs to Know." International City/County Management Association (ICMA). http://www.icma.org/docs/500622.htm. [2002-OCT-30]
Steps city managers can take in evaluating and coordinating response to a terrorist threat.

"Regional Emergency Coordination Plan." Metropolitan Washington Council of Governments. Support Function 2, "Communications Infrastructure." http://www.mwcog.org/homeland_plan/RESF_download.htm. [2002-OCT-30]
Case example of Washington Metro area emergency communications compatibility.

"Regional Emergency Preparedness Contacts: Safeguarding the Nation's Communities." Alliance for Regional Stewardship. March 2002. http://www.regionalstewardship.org/Documents/REPCSReport.pdf. [2002-OCT-30]
Report on state/regional emergency preparedness, training, and community collaboration. Provides numerous local government case examples.

"State, Local and Private Sector Coordination." White House Office of Homeland Security. http://www.whitehouse.gov/deptofhomeland/sect7.html. [2002-OCT-30]
Describes how the new Dept. of Homeland security would strengthen interoperability.

State and Local Domestic Preparedness Support Helpline. U.S. Dept of Justice. http://www.ojp.usdoj.gov/odp/docs/helpline.htm [2002-OCT-30]

"Trends in State Terrorism Preparedness." National Emergency Management Association. http://www.nemaweb.org/Trends_in_Terrorism_Preparedness/index.htm. [2002-OCT-30]
Report on state departments of homeland security and their overall effect on preparedness and capabilities.

Federal Communications Commission, Wireless Telecommunications Bureau, Public Safety and Private Wireless Division. http://www.fcc.gov/wtb/publicsafety. [2002-OCT-30]
Information on spectrum-related issues, hot topics, regulatory actions and decisions, Public Safety Wireless Advisory Committee reports, regional plan action, radio services and licensing, frequency coordination, spectrum refarming, and FCC rules.

National Telecommunications and Information Administration, U.S. Department of Commerce. http://pswac.ntia.doc.gov/pubsafe/index.html. [2002-OCT-30]
Information on public safety-related spectrum and telecommunications programs within the Federal Government, Public Safety Wireless Advisory Committee reports, and Telecommunications and Information Infrastructure Assistance Program grants.

National Public Safety Telecommunications Council. http://rmlectc.dri.du.edu/npstc. [2002-OCT-30]Information on issues related to public safety telecommunications activities, including the availability of spectrum for public safety communications and spectrum licensing.

National Institute of Justice, National Law Enforcement and Corrections Technology Center, U.S. Department of Justice. http://www.nlectc.org. [2002-OCT-30]
Studies, reports, or a video ("*Why Can't We Talk*?" NCJ-172213) related to public safety radio spectrum and interoperability issues.

Public Safety Wireless Network Program. http://www.pswn.gov. [2002-OCT-30]
Information regarding public safety communications interoperability and wireless communications systems planning and implementation

6. Training

There's no way around it: in the event of a terrorist incident, local responders will get there first. And that means they need comprehensive training in what to do, particularly in the event of a radiological, chemical, or biological attack.

At Issue

Why Training? The National League of Cities' Working Group on Homeland Security developed a list of 12 lessons based on a series of briefings held with key responders to the September 11, 2001, attacks on the World Trade Center. The lessons are intended to offer practical guidance to local officials in cities and towns of all sizes as they develop and refine local and regional homeland security plans. Among the lessons was the following:

> *Emphasize training and cross training for all personnel.* Broad cross training will increase the likelihood that someone on site knows what to do even if the "right people" are not there at every moment. Training should also focus on using discretion, common sense, and good judgment during an emergency so that employees have the confidence and skill to act quickly and responsibly in stressful situations.

According to the NLC Working Group, training and practice are the only way to make a city or town's emergency plan part of everyday business—not only for first responders but also for top officials and employees at all levels of government. Training and practice sessions also are a practical and efficient way to identify and resolve procedural difficulties while always striving to improve the plan.

For the complete list of lessons learned, see
http://www.nlc.org/nlc_org/site/newsroom/terrorism_response/lessons_learned.cfm

What Responders Need to Know. In August 2002, the Office of Domestic Preparedness of the U.S. Department of Justice issued a publication, *Emergency Responder Guidelines*, that paints a comprehensive picture of the training that is necessary for fire, police and other personnel to respond effectively and safely to an act of terrorism involving the use of weapons of mass destruction.

The guidelines identify three training levels—Awareness, Performance, and Planning and Management—that should guide the provision and acquisition of training. Within each training level, the document lays out a comprehensive set of guidelines for employees in the key "response disciplines" (e.g., law enforcement, fire, EMS, etc.).

Reviewing the awareness training guidelines for law enforcement officers alone provides an indication of the broad scope that training must take:

Awareness Level Guidelines—Law Enforcement

1. **Recognize hazardous materials incidents.** The law enforcement officer should:

    a. Understand what hazardous materials are, as well as the risks associated with these materials in an emergency incident or event.
    b. Identify if hazardous materials are present in an emergency incident or event.
    c. Know how to use the *North American Emergency Response Guidebook* (NAERG) published by the U.S. Department of Transportation.
    d. Use the NAERG (or other available resources) to identify the hazardous material.
    e. Understand the potential outcomes or consequences of an emergency due to the presence of hazardous materials.

2. **Know the protocols used to detect the potential presence of weapons of mass destruction (WMD) agents or materials**. The law enforcement officer should:

    a. Understand what WMD agents or materials are and the risks associated with these materials in an emergency incident or event.
    b. Know the indicators and effects of WMD on individuals and property. Be able to recognize signs and symptoms common to initial victims of a WMD-related incident or event. Know the physical characteristics or properties of WMD agents or materials that could be reported by victims or other persons at the scene.
    c. Be familiar with the potential use and means of delivery of WMD agents or materials.
    d. Know locations or properties that could become targets for persons using WMD agents or materials.
    e. Recognize unusual trends or characteristics that might indicate an incident or event involving WMD agents or materials.

3. **Know and follow self-protection measures for WMD events and hazardous materials events**. The law enforcement officer should:

    a. Understand the hazards and risks to individuals and property associated with WMD agents and hazardous materials. Recognize the signs and symptoms of exposure to WMD agents and hazardous materials.
    b. Know how to use, inspect, and properly maintain the personal protective equipment issued to the officer. Understand the limitations of this equipment in protecting someone exposed to WMD agents or hazardous materials.
    c. Understand that ambulatory victims should move upwind and upgrade from the area. Know that potentially contaminated victims should be isolated from others. These victims should be advised about appropriate actions to take and that they may need to be decontaminated. Minimize contamination of adjacent areas.
    d. Understand the role of the first responder as well as other levels of response in the department's emergency response plan.
    e. Be familiar with his/her agency's emergency response plan and procedures. Understand the individual officers' role in those procedures.
    f. Know what defensive measures to take during a WMD or hazardous materials incident or event to help ensure personal and community safety. These measures may include maximizing the distance between the officer and hot zone, using shielding

such as solid walls for protection, minimizing personal exposure time to agents or materials that might be found in the warm zone or within the plume, and moving upgrade and upwind.

4. Know procedures for protecting a potential crime scene. The law enforcement officer should:

a. Understand and implement procedures for protecting evidence and minimizing disturbance of the potential crime scene while protecting others. Understand the roles, responsibilities, and jurisdictions of Federal agencies related to a WMD event or incident.
b. Recognize the importance of crime scene preservation and initiate measures to secure the scene.
c. Protect physical evidence such as footprints, relevant containers, or wrapping paper, etc.
d. Advise witnesses and bystanders who may have information to remain at the scene in a safe location until they have been interviewed and released. Be aware of people arriving or departing the scene. Note license plate numbers or other relevant data. Question the caller, witness(es), or victim(s) to obtain critical information regarding the incident or event. Such questions include, "Where is the package, and what does it contain?" "Does the package have an unusual odor or smell?" "Has the package been disturbed?" "Have there been any threats received before receipt of the package" "Does the package contain a written threat, and if so, what does it say?"

5. Know and follow agency/organization's scene security and control procedures for WMD and hazardous material events. The law enforcement officer should:

a. Understand his/her agency/organization's site security and scene control procedures for awareness level trained personnel. Follow these procedures for ensuring scene security and for keeping unauthorized persons away from the scene and adjacent hazardous areas. Such procedures include cordoning off the area to prevent anyone from inadvertently entering the scene. Maintain scene security and control until a higher authority arrives at the scene.
b. Be familiar with his/her agency's incident command procedures.
c. Protect physical evidence such as footprints, relevant containers, or wrapping paper, etc.
d. Know and follow his/her agency's procedures for isolating the danger area. Know how to deal with contaminated victims until a higher authority arrives.
e. Recognize that the incident or event scene may be a crime scene and that evidence must be protected and undisturbed until a higher authority arrives and takes control.

6. Possess and know how to properly use equipment to contact dispatcher or higher authorities to report information collected at the scene and to request additional assistance or emergency response personnel. The law enforcement officer should:

a. Know how to use communications equipment, including a two-way radio or cellular phone to contact the dispatcher or higher authorities to apprise them of the situation at

the scene and to request additional assistance and personnel to properly deal with the event.

b. Understand how to accurately describe a WMD event and be aware of the available response assets within the affected jurisdiction(s) nearest the event location.
c. Know when to request additional help and follow his/her agency's emergency response plan procedures for establishing incident command.
d. Know how to notify the communications center or dispatcher and to assess the degree of hazard to obtain appropriate additional resources.

The ODP document lists similar guidelines for other responders in the areas of awareness, performance, and planning and management. For the complete document, see http://www.ojp.usdoj.gov/odp/docs/EmergencyRespGuidelinesRevB.pdf

The Role of Cross-Training. Experts and practitioners alike recognize the importance of cross-training in preparing police, fire, EMS, and other personnel to respond effectively to a terrorist attack. For example, in the event that firefighters are the only personnel able to reach the victims, they will need to possess medical skills so that victims can be properly cared for in the immediate aftermath of an attack. They must also be able to monitor and detect hazardous substances, decontaminate victims, and protect themselves and the public from further exposure.

Ideas for Local Action

Access Training Resources. In response to the multitude of demands that a terrorist attack would place on local first responders, federal, state and other agencies are developing a range of training and information resources.

In addition to the multiple resources found in this document, please refer to NLC's *Homeland Security: Federal Resources for Local Governments*. This reference guide is posted on NLC's website as a working document to provide local elected officials with the latest information on the programs and resources available at the federal level to help municipalities prepare for and respond to threats of terrorism. Appendix C to that report contains a list of training courses available across the country for first responders and incident managers. Included below is summary of some of those available programs, along with URLs and contact numbers.

Resources

Federal Emergency Management Agency(FEMA)/National Fire Academy 301-447-1333
http://www.usfa.fema.gov/dhtml/fire-service/nfa-on.cfm [2002-NOV-18]
http://www.usfa.fema.gov/dhtml/fire-service/nfa-off.cfm [2002-NOV-18]
http://www.usfa.fema.gov/dhtml/fire-service/nfa-train.cfm [2002-NOV-18]

FEMA/Emergency Management Institute 540-542-2548
http://training.fema.gov/EMIWeb/ctrt.htm [2002-NOV-18]

FEMA/Chemical Stockpile Emergency Preparedness Program (CSEPP) 202-646-2734
http://www.fema.gov/rrr/csepp2.shtm#top [2002-NOV-18]

Department of Health and Human Services (DHHS)/Office of the Assistant Secretary for Public Health/ Emergency Preparedness (OPHEP) 256-820-9135 http://ndms.dhhs.gov/ [2002-NOV-18]

DHHS/ Health Resources & Services Administration (HRSA)/The Public Health Training Center Program 888-ASK-HRSA.
http://www.hrsa.gov/terrorism/hrsa_public_health_training_cent.htm [2002-NOV-18]

Centers for Disease Control/Division of Laboratory Systems/National Laboratory Training Network (NLTN) 800-536-6586 http://www.phppo.cdc.gov/nltn/default.asp [2002-NOV-18]

Environmental Protection Agency (EPA) 513-251-7669
http://www.epa.gov/superfund/programs/er/hazsubs/index.htm [2002-NOV-18]
http://www.epa.gov/radiation/rert/prepare.htm#training [2002-NOV-18]
http://www.epa.gov/superfund/programs/er/index.htm [2002-NOV-18]

U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) 301-447-1333
http://www.usamriid.army.mil/education/index.html [2002-NOV-18]

U.S. Army Medical Research Institute of Chemical Defense (MRICD) 410-671-2230
http://chemdef.apgea.army.mil/ [2002-NOV-18]

U.S. Army Chemical School 573-563-7257 http://www.wood.army.mil/usacmls/ [2002-NOV-18]

U.S. Army Office of the Surgeon General (OTSG) (USAMRIID) 301-619-4535
http://hld.sbccom.army.mil/ps/ps_wmd_ip.htm [2002-NOV-18]

Department of Defense U.S. Army Soldier & Biological Chemical Command 800-368-6498
http://hld.sbccom.army.mil/ [2002-NOV-18]

Department of Energy (DOE) Radiation Emergency Assistance Center and Training Site (REAC/TS)
423-576-4872 http://tis.eh.doe.gov/training/ [2002-NOV-18]

DOE/IAFF Training for Radiation Emergencies 423-576-3388
http://dewey.tis.eh.doe.gov/fire/fro/fro.html [2002-NOV-18]

Department of Justice/Office of Justice Programs 615-399-9908
http://www.ojp.usdoj.gov/terrorism/technical_assistance.htm [2002-NOV-18]

Department of Transportation 617-494-2206 http://www.tsi.dot.gov/ [2002-NOV-18]

Armed Forces Radiobiology Research Institute (AFFRI)/Uniformed Services
http://www.afrri.usuhs.mil/ [2002-NOV-18]

University of the Health Sciences (USUHS) 301-295-0316 http://rad.usuhs.mil/ [2002-NOV-18]

7. Crisis Communications

In the event of a terrorist attack, one of the most important jobs of local elected officials is to provide the public with reliable information about what happened, what people can do to protect themselves and their families, and how the government is responding.

At Issue

The Human Dimension of Terrorism. In *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, a special committee appointed by the National Research Council of the National Academies concludes that there is a "human dimension" to every type of terrorist attack. As much as they may want to destroy buildings and infrastructure, the main goal of terrorists is to generate "behavioral, attitudinal, and emotional responses" in the populations they target.

As a result, according to *Making the Nation Safer*, one way for local officials to blunt the effects of terrorism is to influence the human response through an effective program of communications.

> "The human response to terrorism can be influenced by such factors as adequacy of preparedness, effectiveness of warnings, and confidence in agencies designated to deal with the crisis."

While government can't completely control how people will react to a terror attack on their city or town, officials can help shape attitudes and behaviors by providing helpful information. Again, from the book:

> "The more information that is made available about how to behave in the event of different kinds of attacks (including readiness training and drills, for example), the more likely it is that people will have a sense of control over uncertain situations and they will be less anxious."

Most important, of course, are communications in the immediate aftermath of a terror event. The authors of *Making the Nation Safer* recommend that governments prepare now to communicate as best they can once an attack occurs. Among the book's recommendations: appropriate and trusted spokespeople should be identified and trained now so that, if a terrorist attack occurs, the government will be prepared to respond not only by supplying emergency services but also by providing important, accurate, and trustworthy information clearly, quickly, and authoritatively.

For the complete text of *Making the Nation Safer*, see
http://books.nap.edu/books/0309084814/html/index.html

The Need for Crisis Communications Planning. Emergency communications should be an essential element of any local emergency response plan. In Polk County, Oregon, officials developed an annex to their Emergency Operations Plan outlining the process for disseminating emergency information and instructions to the public during periods of disaster. The

assumptions behind the plan can provide guidance to other local officials as they consider how to plan their emergency communications activities. These assumptions are as follows:

1. An effective program combining both education and emergency information can significantly reduce disaster-related casualties and property damage.
2. Both the media and the public will expect and demand that information about an emergency be provided in a timely manner.
3. The local media, particularly radio and television, can perform an essential role in providing emergency instructions and status information to the public, both through news bulletins and Emergency Alert System (EAS) broadcasts. (See sidebar for more on the EAS.)
4. Demand for information during a disaster can be overwhelming if sufficient trained staff are not available.

For the complete Polk County plan, see http://www.co.polk.or.us/PDFs/Sheriff/EOP.pdf

About the Emergency Alert System

The Emergency Alert System (EAS) was established by the Federal Communications Commission (FCC) in November 1994. It replaced the Emergency Broadcast System (EBS) as a tool that the President and other officials at the state and local levels can use to warn the public about emergency situations.

Using digital technology to distribute emergency messages, the EAS provides state and local officials with a way to quickly send out important local emergency information targeted to a specific area. The EAS digital system architecture allows broadcast stations, cable systems, participating satellite companies, and other services to send and receive emergency information quickly and automatically even if those facilities are unattended.

For more on the EAS, see the FCC's special website, http://www.fcc.gov/eb/eas/

Ideas for Local Action

Informing the Public: Seven Cardinal Rules. In 1988, the U.S. Environmental Protection Agency issued a publication, *Seven Cardinal Rules of Risk Communication*, that provides local officials and others with a concise set of guidelines for keeping the public informed in crisis situations such as terrorist attacks. The rules laid out in the publication are as follows:

1. *Accept and involve the public as a partner.* Your goal is to produce an informed public, not to defuse public concerns or replace actions.

2. *Plan carefully and evaluate your efforts.* Different goals, audiences, and media require different actions.

3. *Listen to the public's specific concerns.* People often care more about trust, credibility, competence, fairness, and empathy than about statistics and details.

4. *Be honest, frank, and open.* Trust and credibility are difficult to obtain; once lost, they are almost impossible to regain.

5. *Work with other credible sources.* Conflicts and disagreements among organizations make communication with the public much more difficult.

6. *Meet the needs of the media.* The media are usually more interested in politics than risk, simplicity than complexity, danger than safety.

7. *Speak clearly and with compassion.* Never let your efforts prevent your acknowledging the tragedy of an illness, injury, or death. People can understand risk information, but they may still not agree with you; some people will not be satisfied.

The Keys to Crisis Communications. In an article prepared for the National Conference of State Legislatures (NCSL), NCSL Public Affairs Officer William Wyatt offers some suggestions for effective crisis communications.

Successful communications, Wyatt writes, depends on several factors, not the least of which is developing a positive communications atmosphere within an organization. That means placing an emphasis on effective communications long before disaster strikes—for example, by making public information officers an integral part of your organization's crisis response planning. That way, everyone involved in the operations will know what to expect from the communications team and vice versa. Similarly, information professionals will know what should be disseminated and what should not.

As important as creating a communications culture is the development of a detailed crisis communications plan, according to Wyatt. He goes on to suggest that the planning effort entail the following steps:

- *Designate a crisis manager*. Appoint someone who will serve as the chief spokesperson to the media and the public. A crisis manager must not only be able to communicate the message effectively, but also should have a level of credibility that is reassuring.

- *Establish lines of communication.* Determine in advance how information will get to the crisis manager, and make sure he or she has access to the best information available.

- *Determine your resources.* Figure out in advance what resources are available to communicate with members of the media, the public, and other key audiences. Which of these resources will reach the most people at once? Do you have capability to provide information in more than one language? Can the internet and e-mail support and broaden your communications effort, and in what ways?

- *Lay it on the table.* When a disaster strikes, the crisis management team is responsible for developing the message that is going to be communicated to the public and the media depending on the crisis. This doesn't mean playing fast and loose with the facts. Quite the opposite, good communication involves laying it all on the table. The public wants to know who, what, when, how, and where. And they want to know as soon as possible.

Once your city or town has a crisis communications plan in place, it is critical that you test it. A dry run, says Wyatt, will allow the communications team to work out the kinks and mend any breaks in the chain of communication while working to decrease overall response time.

Wyatt concludes by observing that the public expects four things from its elected leaders: openness, accessibility, responsiveness, and trust. During a crisis, it is critical that these qualities drive the information that gets to the public.

From the complete article, see: http://www.ncsl.org/programs/legman/nlssa/402crisis.htm

Working with the Media

"I would encourage any community that is confronted with a crisis … to understand that the news media can be an absolute help in a crisis such as this. We made a point from the very beginning of this crisis to keep our community as informed as we possibly could, sharing with them whatever information we got, essentially as soon as we got it. And by doing that, I believe we kept our community calm."

-- Glen Gilmore, Mayor of Hamilton Township, New Jersey, reflecting on his government's activities in the immediate aftermath of the September 11, 2001, attacks. (From "Protecting the Homeland Through Executive Leadership and Effective Communications," a CXO Media Policy Forum. http://www.cio.com/forum3/tips.pdf)

Creating a Joint Information Center. The International Association of Emergency Managers (IAEM) advises that local governments establish a Joint Information Center (JIC) to ensure a timely flow of reliable information to all key audiences. The JIC is a coordinated and centralized information repository that can serve as the central location for conducting briefings by relevant officials. Ideally, according to the IAEM, the JIC should have representation from each component entity (at all levels of government) that is contributing to the response effort. For more, see http://www.iaem.com/Emergency_Response_Info.doc

Communicating with Schools. In the event of a terror attack, your government has a special responsibility to work with school officials to ensure that local children are receiving age-appropriate information about what happened and how to respond. The following advisory issued to New York schools on September 11, 2001, by the state Commissioner of Education, Richard P. Mills, provides some guidelines for city and school officials to consider in your crisis communications planning.

Crisis Advisory for Schools—September 11, 2001

- Follow your district and school crisis plan.
- Preference is to keep schools open. To try to keep life as normal as possible for students.
- Stay as calm as possible. Adults need to be role models for children.
- Encourage communication opportunities in classrooms. Let students/adults talk about their feelings.

- Try to send positive messages to staff that they have the skills to handle this crisis. However, there may be adults who struggle with this task. Make plans to support these staff. (Make use of your own school health services staff.)
- Communicate to students that the adults are doing everything they can to keep students safe. BE VERY HONEST. *Do not* make promises you cannot keep.
- Be sensitive/accommodate the needs of students, parents, staff (when school is staying open, support parents who choose to keep students home).
- It is important for you to consider sending a message home to parents today.

Resources

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Committee on Science and Technology for Countering Terrorism, National Research Council. http://books.nap.edu/books/0309084814/html/index.html. [2002-NOV-11]
Online publication touching on all aspects of terrorism prevention and response, including crisis communications.

The Emergency Alert System (EAS) Homepage. Federal Communications Commission. http://www.fcc.gov/eb/eas/. [2002-NOV-11]
Information and links related to the EAS.

"Be Prepared: Communicating in a Crisis" by William Wyatt. National Conference of State Legislatures. http://www.ncsl.org/programs/legman/nlssa/402crisis.htm. [2002-NOV-11]
Article offering suggestions for effective crisis communications.

"Crisis Communications Tips from the Experts." http://www.cio.com/forum3/tips.pdf. [2002-NOV-11]Information and excerpts from the CXO Media Policy Forum, "Protecting the Homeland Through Executive Leadership and Effective Communications."

"Emergency Response Information." International Association of Emergency Managers. http://www.iaem.com/Emergency_Response_Info.doc. [2002-NOV-11]
Basic information on crisis communications.

Health Alert Network, Centers for Disease Control. http://www.phppo.cdc.gov/han/. [2002-NOV-11]
Homepage of project designed to ensure communications capacity at local and state health departments.

"Talking About Disaster." The American Red Cross. http://www.redcross.org/disaster/safety/guide.html. [2002-NOV-11]
Guidebook developed to assist anyone providing disaster safety information to the public.

"Model Emergency Response Communications Plan for Infectious Disease Outbreaks and Bioterrorist Events." The Association of State and Territorial Directors of Health Promotion and

Public Health Education (ASTDHPPHE), May 2000.
http://www.astdhpphe.org/bioterr/bioterror.pdf. [2002-NOV-11]

"The News Media's Vital Role in Chemical Emergency Planning and Response." Chemical Education Foundation. http://www.chemed.org/publicat/Bulletins/stew22/bulletin22.pdf [2002-NOV-11]
Article about how the media can help keep the public informed in the event of a chemical emergency.

"A Primer on Health Risk Communication Principles and Practices." Agency for Toxic Substances and Disease Registry. http://www.atsdr.cdc.gov/HEC/primer.html. [2002-NOV-11]
The basics on risk communication from the federal government.

Appendix A: Comprehensive List of All Resources in Part One

City Response to Terrorism and Disaster. Lexington, KY: Kentucky League of Cities. 2002. www.klc.org/terrorism2.htm [2002-SEP-06].
This guide provides step-by-step advice on how to create and maintain a comprehensive emergency management program and includes the steps in the planning process, emergency management considerations, and hazard-specific information.

Community Response to the Threat of Terrorism. Fairfax, VA: Public Entity Risk Institute. November 2001. http://www.riskinstitute.org/ptrdocs/CommunityResponse-Terrorism.pdf [2002-AUG-15].
This collection of papers provides practical ideas on local government emergency preparedness.

"Comprehensive Exercise Program." Federal Emergency Management Agency. www.fema.gov/rrr/cepnew.shtm [2002-AUG-26].
Through training and disaster drills, the Comprehensive Exercise Program (CEP) improves the proficiency of federal, state, and local governments to perform emergency management functions in an efficient and timely manner.

"Disaster Mental Health: Tips for Talking About Disasters." U.S. Department of Health and Human Services. www.mentalhealth.org/cmhs/emergencyservices/after.asp [2002-SEP-03].
This Web page provides links to sites that focus on disaster mental health for adults, children, and disaster response workers. It also links to Spanish-language sites.

"Education and Training." Federal Emergency Management Agency. www.fema.gov/tab_education.shtm [2002-AUG-26].
FEMA provides many programs, courses, and materials to support emergency preparedness and response for emergency personnel as well as the general public.

"Emergency Preparedness and Response." (July 2002). The White House. www.whitehouse.gov/homeland/book/sect3-5.pdf [2002-AUG-22].
A chapter from the National Strategy for Homeland Security, this document discusses a variety of steps the federal government must take to plan and prepare for large-scale terrorist incidents, including support for local first responders.

"Emergency Readiness Issues Intersection." Washington, DC: International City/County Management Association. http://icma.org/issueintersections/er.cfm [2002-AUG-15].
This Web page contains links to dozens of documents on planning for emergency situations, including sample plans from cities across the United States.

"Emergency Readiness: Citizen Guides" International City/County Management Association. www.icma.org/issueintersections/dsp_ER.cfm?SubCategory_Name=Citizen%20Guides%20for%20Emergency%20Preparedness [2002-AUG-26].
This collection of citizen guides for emergency preparedness includes 20 examples, most of them developed by local governments.

"Emergency Readiness: Media Relations" International City/County Management Association. www.icma.org/issueintersections/dsp_ER.cfm?SubCategory_Name=Media%20Relations%20in%20Emergency%20Situations [2002-AUG-26]
This page provides information on media relations in emergency situations for local governments.

"Emergency Responder Guidelines." (August 1, 2002). U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/docs/EmergencyRespGuidelinesRevB.pdf [2002-AUG-22].
Intended for first responders, this document provides baseline information on the training necessary to respond to an act of terrorism using weapons of mass destruction.

"Emergency Response Information." International Association of Emergency Managers. www.iaem.com/Emergency_Response_Info.doc [2002-AUG-26].
IAEM presents ideas on emergency response information and communication in its working document, "IAEM Terrorism Program Guide."

"Emergency Response to Terrorism: Self-Study (ERT:SS) (Q534)." Federal Emergency Management Agency. www.usfa.fema.gov/dhtml/fire-service/nfa-off3ss2.cfm [2002-AUG-26].
This page provides access to a free, 10-hour, self-paced course designed to provide basic awareness training to prepare first responders for terrorist incidents. Students who successfully complete the exam will be eligible for a National Fire Academy certificate of training.

"Equipment Acquisition Grants." U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/grants/goals.htm [2002-AUG-22].
This page describes the ODP Equipment Grant Program, which provides funding to enhance the capacity of state and local jurisdictions to respond to incidents of domestic terrorism using weapons of mass destruction.

"Exercises." U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/exercises/state.htm [2002-AUG-22].
This page describes the ODP's State and Local Domestic Preparedness Exercise Program and aids states and local jurisdictions in advancing domestic preparedness through evaluation of authorities, plans, policies, procedures, protocols, and response resources.

"Facing the Future: How Should We Move Forward After September 11?" Study Circles Resource Center. www.studycircles.org/pages/issues/americaresponds.html [2002-AUG-26].
This site promotes the benefits of engaging citizens in discussions about homeland security through study circles. A study circle is a small group of people from different backgrounds and viewpoints who meet several times to talk about an issue.

"Field Office Information." Federal Bureau of Investigation. www.fbi.gov/contact/fo/info.htm [2002-AUG-22].
This page provides links to FBI field offices in cities across the country. The list is sorted alphabetically by city name.

Guide for All-Hazard Emergency Operations Planning: State and Local Guide (101). (September 1996). Federal Emergency Management Agency. www.fema.gov/rrr/gaheop.shtm [2002-AUG-26].
This document is a comprehensive guide to emergency planning for local officials.

Guide for All-Hazard Emergency Operations Planning: State and Local Guide (101) Chapter 5, Attachment B -- Communications. (September 1996). Federal Emergency Management Agency. www.fema.gov/pdf/rrr/5-ch-b.pdf [2002-AUG-26].
The purpose of Attachment B is to provide details necessary for understanding total emergency communications plans.

Guide for All-Hazard Emergency Operations Planning: State and Local Guide (101) Chapter 6, Attachment G -- Terrorism. (September 1996). Federal Emergency Management Agency. www.fema.gov/rrr/allhzpln.shtm [2002-AUG-26].
The purpose of Attachment G is to aid state and local emergency planners in developing and maintaining a Terrorist Incident Appendix (TIA) to an Emergency Operations Plan (EOP) for incidents involving terrorist-initiated weapons of mass destruction (WMD).

"Homeland Security State Contact List" The White House. www.whitehouse.gov/homeland/contactmap.html [2002-AUG-22].
A clickable map lets you select your state to see who the governor has appointed as the homeland security contact.

"Information Sharing and Systems" (July 2002). The White House. www.whitehouse.gov/homeland/book/sect4-2.pdf [2002-AUG-22].
A chapter from the National Strategy for Homeland Security, this document discusses integrating communications and information sharing among all levels of government and the private sector. It also calls for adopting data standards.

"Leadership Training Institute." National League of Cities. www.nlc.org/nlc_org/site/programs/training_and_education/index.cfm [2002-AUG-2002]
NLC's Leadership Training Institute offers courses on media relations for local elected officials.

LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan. (August 2001). U.S. Environmental Protection Agency. www.epa.gov/ceppo/factsheets/lepcct.pdf [2002-AUG-22].
This document addresses the increased threats of biological or chemical terrorism in the U.S. and what local environmental planning committees (LEPCs) can do to prepare for and respond to them.

"Managing the Threat of Terrorism." Washington, DC: International City/County Management Association. ICMA IQ Report. December 2001.
This report explores what communities can do to prevent, prepare for, and respond to terrorist attacks—using both traditional and nontraditional methods of dealing with disasters

"National Crime Prevention Council." Washington, DC: National Crime Prevention Council. www.ncpc.org [2002-SEP-06].
This is the home page of the organization and includes links to community-based prevention programs, ideas for neighborhood action, and a crime prevention library.

"National Crime Prevention Council: Neighborhood Action." Washington, DC: National Crime Prevention Council. www.ncpc.org/neigh.htm [2002-SEP-06].
This page has a variety of links to information on topics like citizen patrols, involving youth, multiculturalism, neighborhood watches, and reaching out to crime victims.

"National Fire Academy." Federal Emergency Management Agency. www.usfa.fema.gov/dhtml/fire-service/nfa.cfm [2002-AUG-26].
This page provides links to courses and programs offered by the National Fire Academy (NFA). The NFA works to enhance the ability of fire and emergency services and allied professionals to deal more effectively with fire and related emergencies.

National Strategy for Homeland Security. (July 2002). The White House. www.whitehouse.gov/homeland/book/nat_strat_hls.pdf [2002-AUG-22].
The purpose of this document is to organize and mobilize the nation to secure the U.S. from terrorist attacks. This is a printable version of the entire 90-page report. Individual chapters of the report may be accessed at www.whitehouse.gov/homeland/book/index.html [2002-AUG-22].

"Needs Assessment and Strategy Development." U.S. Department of Justice, Office for Domestic Preparedness. https://grants2.ojp.usdoj.gov/servletext/OS_localJur_index [2002-AUG-22].
Local governments may download the "Assessment and Strategy Development Toolkit" from this page. Assessments ensure that measures taken to reduce vulnerabilities are justifiable and that ODP grants are appropriately targeted to address identified risks and requirements.

"ODP Weapons of Mass Destruction Training Program Course Catalog." U.S. Department of Justice, Office for Domestic Preparedness. http://www.ojp.usdoj.gov/odp/docs/coursecatalog.pdf [2002-AUG-22].
This catalog is designed to provide emergency response personnel with comprehensive information regarding training courses and technical assistance offered by ODP.

"Oklahoma City - Seven Years Later: Lessons for Other Communities." Oklahoma City, OK: Oklahoma City National Memorial Institute for the Prevention of Terrorism. 2002.
Chapter 3 focuses on local and state government planning for and response to terrorist incidents.

"Organizing for a Secure Homeland." (July 2002). The White House. www.whitehouse.gov/homeland/book/sect2-2.pdf [2002-AUG-22].
A chapter from the National Strategy for Homeland Security, this document discusses local governments' roles in homeland security efforts and coordination among all levels of government.

"Overview: Training and Technical Assistance." U.S. Department of Justice, Office for Domestic Preparedness. www.ojp.usdoj.gov/odp/ta/overview.htm [2002-AUG-22].
This page describes the ODP's State and Local Domestic Preparedness Training and Technical Assistance Program and provides links to more detailed information. The program provides direct training and technical assistance to state and local jurisdictions to enhance their capacity and preparedness to respond to domestic incidents.

"Planning for Disaster Recovery." The International City/County Management Association (ICMA). First printed in 1993, this 24-page report provides case studies of the disaster recovery process and discusses problems, resources, and solutions. The report is still available—call ICMA at 800-745-8780 and ask for item #40834.

"Preparing for Terrorism: What Every Manager Needs to Know" by Howard Levitin. Washington, DC: International City/County Management Association. Public Management. December 1998.
http://icma.org/documents/index.cfm?code=%2A%2B%40%5C%23WUDM75%3C%2AGM%20%2A%0A&hdr=II [2002-AUG-15].
This pre-9/11 article discusses the reasons for implementing an emergency plan, and suggests first steps toward preparedness.

"Risk Management Primer for Small Town and Township Officials." Public Entity Risk Institute. www.riskinstitute.org/project.asp?item_id=1006 [2002-SEP-03]
Scheduled for release in late fall 2002, this primer is designed to introduce small town leaders to key considerations in managing overall risks in their jurisdictions. It includes a community risk management checklist, types of insurance coverage available, and what the insurance does and does not cover. The primer was developed by the National Center for Small Communities, through a project funded by a grant from PERI. The primer will be available on the NCSC website, www.smallcommunities.org.

"State Departments, Divisions of Insurance." Risk Management Resource Center. www.eriskcenter.org/statelocal/department/dept_ddi.html [2002-SEP-03].
This site provides links to the insurance regulation departments of all 50 states.

"Symposium Center/About PERI Symposium Programs." Public Entity Risk Institute. www.riskinstitute.org/symposium.asp [2002-AUG-26].
This site lists the Public Entity Risk Institute's symposiums and issue papers, which are designed to provide municipal officials with information on risk assessment and emergency planning.

"Terrorism in America: Seven Preventative Steps for Every Municipal Employer" by Mark J. Neuberger. Washington, DC: International Municipal Lawyers Association. Municipal Lawyer. May/June 2002.
This article emphasizes the importance of a disaster recovery plan in your city and the necessary steps to develop it.

Terrorism Program Guide (draft). Falls Church, VA: International Association of Emergency Managers. March 2002. www.iaem.com/terrorism_program_guide_.html [2002-AUG-15].
This draft document offers detailed information on emergency planning, including organizing and setting priorities to develop a plan.

United for a Stronger America: Citizens' Preparedness Guide. (January 2002). Washington, DC: National Crime Prevention Council. www.weprevent.org/usa/cover.pdf [2002-SEP-06]. This guide provides suggestions for citizens on preparedness in their homes, neighborhoods, schools, workplaces, places of worship, and public areas.

"What is Being Done to Protect the Nation's Water Infrastructure?" U.S. Environmental Protection Agency. www.epa.gov/safewater/security/index.html [2002-AUG-22]. This page provides links to security strategies for small/medium water utilities, grants for publicly-owned drinking water utilities, vulnerability assessment resources, and training resources.

Appendix B: Comprehensive List of All Resources in Part Two

"21st Century Guide to Bioterrorism, Biological and Chemical Weapons, Germs and Germ Warfare, Nuclear and Radiation Terrorism." Naval Operational Medical Institute. http://forum.nomi.med.navy.mil/cd/CD085/09%20p2%20NBC%20TERRORISM%20GUIDE/contents.PDF. [2002-OCT-25]
List of terrorism links from a government standpoint. Includes reports, and information on training, prevention, and identifying the threat.

"A National Teleconference on Bioterrorism: Lessons and Practices in Cooperative Planning for Bioterrorist Events." The Council on State Governments. http://www.csg.org/bioterrorismteleconference.htm. [2002-OCT-25]
Transcript of a teleconference on state-local cooperation in addressing the threat of bioterrorism.

"A Primer on Health Risk Communication Principles and Practices." Agency for Toxic Substances and Disease Registry. http://www.atsdr.cdc.gov/HEC/primer.html. [2002-NOV-11]
The basics on risk communication from the federal government.

"Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." http://www.nautilus.org/info-policy/workshop/papers/denning.html. [2002-NOV-01]
Historical examples of cyberterrorism and hacking for foreign policy intelligence, and an outline of the threat today.

"Additional Resources [on Bioterrorism]." National Association of City and County Health Officials (NACCHO). http://www.naccho.org/general500.cfm. [2002-OCT-25]
Includes Articles, organizational links, training and coursework, and other resources.

"Advice for Securing Buildings against a chemical or biological attack." Lawrence Berkeley National Laboratory. http://securebuildings.lbl.gov/. [2002-OCT-25]
Prevention advice and training tips.

"Advisories on Anthrax, Mail, and Related Topics." Chemical and Biological Defense Information Analysis Center.
http://www.cbiac.apgea.army.mil/resources/directory/anthrax_info.htm. [2002-OCT-25]
Numerous resources for a wide range of topics related to biological and chemical terrorism.

Armed Forces Radiobiology Research Institute (AFFRI)/Uniformed Serviceshttp://www.afrri.usuhs.mil/ [2002-NOV-18]

"Be Prepared: Communicating in a Crisis" by William Wyatt. National Conference of State Legislatures. http://www.ncsl.org/programs/legman/nlssa/402crisis.htm. [2002-NOV-11]
Article offering suggestions for effective crisis communications.

"Biological and Chemical Weapons." National Institute of Health: MEDLine Plus.
http://www.nlm.nih.gov/medlineplus/biologicalandchemicalweapons.html. [2002-OCT-25]
Contains a wide range of health related information.

"Bioterrorism – A threat Without Borders." Council on State Governments. http://stars.csg.org/sgn/2002/february/0202sgn_18.pdf. [2002-OCT-25]
Key issues on bioterrorism preparedness, as well as model state homeland security initiatives.

"Bioterrorism and Local Public Health Case Examples from Recent Anthrax Events Summary." NACCHO. http://www.naccho.org/general456.cfm. [2002-OCT-25]
"Best Practices" examples from a discussion among local officials on dealing with the Anthrax situation following the Sept. 11 attacks.

"Bioterrorism-Related Anthrax." Centers for Disease Control and Prevention. http://www.cdc.gov/ncidod/eid/index.htm. [2002-OCT-25]
Numerous articles on Anthrax detection, prevention, research.

Center for Civilian Biodefense Strategies. http://www.hopkins-biodefense.org/ [2002-OCT-25]
"Countering Bioterrorism and Other Threats to the Food Supply." Foodsafety.gov. http://www.foodsafety.gov/~fsg/bioterr.html. [2002-OCT-25]
Portal site to federal resources regarding food safety (Agroterrorism).

Centers for Disease Control/Division of Laboratory Systems/National Laboratory Training Network (NLTN) 800-536-6586 http://www.phppo.cdc.gov/nltn/default.asp [2002-NOV-18]

"The Challenge of Cyberterrorism." Public Entity Risk Institute. http://www.riskinstitute.org/lib_art.asp?art_id=1014. [2002-NOV-01]
Article about attack methods, potential targets, the future, and preparedness.

"Chemical and Biological Terrorism." Public Entity Risk Institute. http://www.riskinstitute.org/lib_art.asp?art_id=1015. [2002-OCT-25]
Describes types of chemical and biological agents, lists examples of local public health initiatives and contains a large list of resources to go to for more help.

"Chemical Emergency." FEMA. http://www.fema.gov/pdf/rrr/talkdiz/chemical.pdf. [2002-OCT-25]
Guidebook for emergency management in case of a major chemical emergency.

"Community Demonstration Project." Federal Geographic Data Committee. http://www.fgdc.gov/nsdi/docs/cdp.html. [2002-OCT-30]
Government pilot project that hopes to show how GIS mapping can solve community problems.

"Chemical Agent Lists and Information." CDC. http://www.bt.cdc.gov/Agent/agentlistchem.asp. [2002-OCT-25]
List of chemical agents commonly found in weapons, links to critical info, emergency procedures.

"Crisis Communications Tips from the Experts." http://www.cio.com/forum3/tips.pdf. [2002-NOV-11]
Information and excerpts from the CXO Media Policy Forum, "Protecting the Homeland Through Executive Leadership and Effective Communications."

"Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study. MIPT. http://www.mipt.org/cbacifindings.asp. [2002-OCT-30]
Discusses chain of command during Oklahoma City Bombing.

Critical Infrastructure Assurance Office. http://www.ciao.gov/. [2002-NOV-01]
Federal Government agency in charge of internet security.

"Cybercare." (July 2002). Journal of Homeland Security.
http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=69 [2002-OCT-25]
Presents a new strategy for mobilizing health care resources in the event of a bioterrorist attack.

"Cyberterrorism and Government Warfare: Government Perspectives." By Michael Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation. http://www.terrorismcentral.com/Library/Teasers/vatis.html. [2002-NOV-01]
Defines the threat of cyberterrorism from the perspective of the FBI.

"The Cyberterrorism Czar – What's Next?" Robert Lemos, CNET.com news.
http://news.com.com/2102-1082-275751.html. [2002-NOV-01]
Article about Richard Clark, Adviser to the President for Cybersecurity.

"Cyberterrorism drill set - Operation Dark Screen to help government, industry prepare for attacks" Federal Computer Week (July 22, 2002).
http://www.globalsecurity.org/org/news/2002/020722-fcw1.htm. [2002-NOV-01]
Information to help people in many arenas better understand their roles in preparing for, recovering from, and protecting the nation's critical infrastructure during a cyberattack.

"Cyberterrorism Resource Center." Global Development Center.
http://www.globaldisaster.org/cyberterrorrescen.shtml. [2002-NOV-01]
Up-to-date news on "cyber-warfare" since the Sept. 11 attacks, also has cyberterrorism resources.

"Cyberterrorism." National Conference of State Legislatures.
http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm. [2002-NOV-01]
Portal site including description of threat, current policy, and resources.

"Cyberterrorism: Fact or Fancy?" FBI Laboratory.
http://www.cs.georgetown.edu/~denning/infosec/pollitt.html. [2002-NOV-01]
This paper discusses the definition of cyberterrorism, its potential, and suggests an approach to the minimization of its' dangers.

"Cyberterrorism…Cybercrime…Cyberwarfare." Center for Strategic and International Studies.
http://www.csis.org/pubs/cyberfor.html. [2002-NOV-01]
Description and history of cyberterrorism, and recommendations.

"Defending America Against Cyberterrorism." ZDNet News. http://zdnet.com.com/2100-1105-531071.html. [2002-NOV-01]
Interview with Richard Clark, adviser to the President for cybersecurity.

Department of Defense U.S. Army Soldier & Biological Chemical Command 800-368-6498 http://hld.sbccom.army.mil/ [2002-NOV-18]

Department of Energy (DOE) Radiation Emergency Assistance Center and Training Site (REAC/TS)423-576-4872 http://tis.eh.doe.gov/training/ [2002-NOV-18]

DOE/IAFF Training for Radiation Emergencies 423-576-3388http://dewey.tis.eh.doe.gov/fire/fro/fro.html [2002-NOV-18]

Department of Health and Human Services (DHHS)/Office of the Assistant Secretary for Public Health/ Emergency Preparedness (OPHEP) 256-820-9135 http://ndms.dhhs.gov/ [2002-NOV-18]

DHHS/ Health Resources & Services Administration (HRSA)/The Public HealthTraining Center Program 888-ASK-HRSA.http://www.hrsa.gov/terrorism/hrsa_public_health_training_cent.htm [2002-NOV-18]

Department of Justice/Office of Justice Programs 615-399-9908http://www.ojp.usdoj.gov/terrorism/technical_assistance.htm [2002-NOV-18]

Department of Transportation 617-494-2206 http://www.tsi.dot.gov/ [2002-NOV-18]

"Dirty Bombs." Council on Foreign Relations. 'Terrorism: Questions and Answers.' http://www.terrorismanswers.com/weapons/dirtybomb2.html. [2002-OCT-30]
Basic information about dirty bombs.

"Disasters Present Health Challenges." (Oct. 2001). Council on State Governments. http://stars.csg.org/sgn/2001/october/1001sgn23.pdf. [2002-OCT-25]
The impact of terrorism on the health care system and tips on how to be prepared.

"Early Warning and Remediation: Minimizing the Threat of Bioterrorism." (April 2002). Journal of Homeland Security.
http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=54 [2002-OCT-25]
Focuses on the early detection of biological agents used as weapons of mass destruction.

"Electronic Crime Publications." National Institute of Justice.
http://www.ojp.usdoj.gov/nij/sciencetech/ecrime_pub.htm. [2002-NOV-01]
List of electronic prime publications, and a searchable abstracts database.

"Electronic Threats and Terroristic Activities." National Conference of State Legislatures.
http://www.ncsl.org/programs/lis/CIP/electerthreat.htm. [2002-OCT-25]
Several states have addressed terrorism in state criminal codes, including statutes that address terroristic activities and threats.

"Elements of Effective Bioterrorism Preparedness." National Association of City and County Health Officials. http://www.naccho.org/files/documents/Final_Effective_Bioterrism.pdf. [2002-OCT-25]
Manual for Local Public Health Officials on how to prepare for a Bioterrorist attack.

The Emergency Alert System (EAS) Homepage. Federal Communications Commission. http://www.fcc.gov/eb/eas/. [2002-NOV-11]
Information and links related to the EAS.

"Emergency Response." CDC. http://www.bt.cdc.gov/emcontact/index.asp. [2002-OCT-25]
Describes who to contact in case of an act of bioterrorism or exposure to chemical/biological agents.

"Emergency Response Information." International Association of Emergency Managers. http://www.iaem.com/Emergency_Response_Info.doc. [2002-NOV-11]
Basic information on crisis communications.

Environmental Protection Agency (EPA) 513-251-7669http://www.epa.gov/superfund/programs/er/hazsubs/index.htm [2002-NOV-18]
http://www.epa.gov/radiation/rert/prepare.htm#training [2002-NOV-18]
http://www.epa.gov/superfund/programs/er/index.htm [2002-NOV-18]

Federal Communications Commission, Wireless Telecommunications Bureau, Public Safety and Private Wireless Division. http://www.fcc.gov/wtb/publicsafety. [2002-OCT-30]
Information on spectrum-related issues, hot topics, regulatory actions and decisions, Public Safety Wireless Advisory Committee reports, regional plan action, radio services and licensing, frequency coordination, spectrum refarming, and FCC rules.

Federal Emergency Management Agency(FEMA)/National Fire Academy 301-447-1333
http://www.usfa.fema.gov/dhtml/fire-service/nfa-on.cfm [2002-NOV-18]
http://www.usfa.fema.gov/dhtml/fire-service/nfa-off.cfm [2002-NOV-18]
http://www.usfa.fema.gov/dhtml/fire-service/nfa-train.cfm [2002-NOV-18]

FEMA/Emergency Management Institute 540-542-2548
http://training.fema.gov/EMIWeb/ctrt.htm [2002-NOV-18]

FEMA/Chemical Stockpile Emergency Preparedness Program (CSEPP) 202-646-2734http://www.fema.gov/rrr/csepp2.shtm#top [2002-NOV-18]

"FBI Briefs Homeland Task Force on Cyberterrorism." National Association of Counties. http://www.naco.org/pubs/cnews/01-12-10/fbi.htm. [2002-NOV-01]
The role of technology in assisting counties to secure America was the theme for the second meeting of the National Association of Counties' Homeland Security Task Force, which gathered Nov. 28 in Santa Fe County, N. M.

"FCC Clears the Air for Safety." Federal Communication Weekly. (June 24, 2002). http://www.fcw.com/supplements/homeland/2002/sup2/hom-wire1-06-24-02.asp. [2002-OCT-30]
News article about FCC's new 700MHz initiative.

"Frequently Asked Questions about Food Safety and Terrorism." U.S. Food and Drug Administration. http://www.cfsan.fda.gov/~dms/fsterrqa.html. [2002-OCT-25]

"The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge." Institute for Security and Intelligence. http://afgen.com/terrorism1.html. [2002-NOV-01]
Insight into cyberterrorists' actions and goals.

"GAO Testimony on Critical Infrastructure Protection." Robert F. Dacey, Director, Information Security Issues, General Accounting Office. [2002-NOV-01]
http://www.terrorismcentral.com/Library/Teasers/GAO.html. Review/oversight hearing for the National Infrastructure Protection Center (NIPC).

"Government Info Sharing Key To Fighting Terrorism." CIO.com.
http://www.cio.com/government/edit/122001_share.html. [2002-NOV-01]
U.S. government officials spoke at a crisis management conference Dec. 18 (2001).

"Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks." May 2002. CDC: National Institute for Occupational Safety and Health.
http://www.cdc.gov/niosh/bldvent/pdfs/2002-139.pdf. [2002-OCT-25]
Specific recommendations on how to protect indoor environments from airborne chemical/biological/radiological agents.

Health Alert Network, Centers for Disease Control. http://www.phppo.cdc.gov/han/. [2002-NOV-11]
Homepage of project designed to ensure communications capacity at local and state health departments.

"Homeland Security and Geographic Information Systems." Federal Geographic Data Committee. http://www.fgdc.gov/publications/homeland.html. [2002-OCT-30]
Information on GIS systems.

"Homeland Security Outlook." American City and County (1 Aug 2002).
http://www.americancityandcounty.com/ar/government_homeland_security_outlook/index.htm. [2002-OCT-30]
Examining local government cooperative agreements and needs for hometown security.

"Interoperability Spectrum Contacts." FCC.
http://wireless.fcc.gov/publicsafety/700MHz/interop-contacts.html. [2002-OCT-30]
State contact info regarding 700MHz radio frequency interoperability.

"Interoperability Spectrum." Federal Communications Commission (FCC).
http://wireless.fcc.gov/publicsafety/700MHz/interop.html. [2002-OCT-30]
Current proceedings, news, FAQ for 700MHz radio frequency for emergency responders.

"Is Cyber Terror Next?" by Dorothy E. Denning, Professor of Computer Science; Director of the Georgetown Institute for Information Assurance, Georgetown University. Social Science Research Council. http://www.ssrc.org/sept11/essays/denning.htm. [2002-NOV-01]
Discusses possibility of a cyberterror attack on the United States.

"Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism." Jan. 1999. National Institute of Justice. http://www.ncjrs.org/pdffiles1/173384.pdf. [2002-NOV-01]
An inventory of State and local law enforcement agencies that is being used to determine the technologies needed by these agencies to combat terrorism.

"LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan." EPA – Chemical Emergency Preparedness and Prevention Office (CEPPO). August 2001. http://yosemite.epa.gov/oswer/ceppoweb.nsf/vwResourcesByFilename/lepcct.pdf/$file/lepcct.pdf [2002-OCT-25]
Information for local governments regarding procedure after a deliberate chemical release.

"Local Government Response to Bioterrorist Attacks." Public Entity Risk Institute (PERI). http://www.riskinstitute.org/lib_art.asp?art_id=1025. [2002-OCT-25]
Extensive list of resources and critical information on how to prepare your city or town.

"Loose Nukes." Council on Foreign Relations. 'Terrorism: Questions and Answers.' http://www.terrorismanswers.com/weapons/loosenukes.html. [2002-OCT-30]
Basic information about loose nuclear weapons.

Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Committee on Science and Technology for Countering Terrorism, National Research Council. http://books.nap.edu/books/0309084814/html/index.html. [2002-NOV-11]
Online publication touching on all aspects of terrorism prevention and response, including crisis communications.

"Managing Hazardous Materials Incidents." CDC. Agency for Toxic Substances and Disease Registry. http://www.atsdr.cdc.gov/mhmi.html. [2002-OCT-25]
A planning guide to help first responders respond to hazardous materials incidents.

"Model Emergency Response Communications Plan for Infectious Disease Outbreaks and Bioterrorist Events." The Association of State and Territorial Directors of Health Promotion and Public Health Education (ASTDHPPHE), May 2000. http://www.astdhpphe.org/bioterr/bioterror.pdf. [2002-NOV-11]

"NACCHO Responds to Bioterrorism." NACCHO. http://www.naccho.org/files/documents/responds_to_bioterrorism.html. [2002-OCT-25]
Links to information on bioterrorism awareness and prevention geared towards local health officials.

National Infrastructure Protection Center. http://www.nipc.gov/. [2002-NOV-01]
The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity.

National Institute of Justice, National Law Enforcement and Corrections Technology Center, U.S. Department of Justice. http://www.nlectc.org. [2002-OCT-30]
Studies, reports, or a video ("*Why Can't We Talk*?" NCJ-172213) related to public safety radio spectrum and interoperability issues.

National Public Safety Telecommunications Council. http://rmlectc.dri.du.edu/npstc. [2002-OCT-30]
Information on issues related to public safety telecommunications activities, including the availability of spectrum for public safety communications and spectrum licensing.

National Telecommunications and Information Administration, U.S. Department of Commerce. http://pswac.ntia.doc.gov/pubsafe/index.html. [2002-OCT-30]
Information on public safety-related spectrum and telecommunications programs within the Federal Government, Public Safety Wireless Advisory Committee reports, and Telecommunications and Information Infrastructure Assistance Program grants.

"National Strategy to Secure Cyberspace." The President's Critical Infrastructure Protection Board. http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html. [2002-NOV-01]
A draft report on the topic from a presidentially appointed panel.

"New York Enlists Private Sector in Fight Against Cyberterrorism." Washington Technology. http://www.washingtontechnology.com/news/1_1/daily_news/17961-1.html. [2002-NOV-01]
Information on how the state of New York protects its information systems and critical infrastructure against terrorist attacks.

"The News Media's Vital Role in Chemical Emergency Planning and Response." Chemical Education Foundation. http://www.chemed.org/publicat/Bulletins/stew22/bulletin22.pdf [2002-NOV-11]
Article about how the media can help keep the public informed in the event of a chemical emergency.

"Nuclear and Radiological Terrorism." Carnegie Endowment for International Peace – Proliferation Brief, 5:14
http://www.ceip.org/files/projects/npp/pdf/Testimony/RoseGsept242002.pdf. [2002-OCT-01]
Testimony before Congress on Sept. 24, 2002 regarding radiological terrorism.

"Nuclear Terrorism: Reactors and Radiological Attacks after September 11." International Atomic Energy Agency.
http://www.iaea.or.at/worldatom/Press/Focus/Nuclear_Terrorism/cameron.pdf. [2002-OCT-30]
Describes in detail the threat of terrorist attacks to nuclear reactors, especially from insiders in a country.

"Oklahoma City – Seven Years Later: Lessons for Other Communities. Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT). http://www.mipt.org/pdf/MIPT-OKC7YearsLater.pdf [2002-OCT-30]

"Other Terrorism." Center for the study of Bioterrorism, Saint Louis University.
http://www.slu.edu/colleges/sph/csbei/bioterrorism/other.htm [2002-OCT-25]
Information on chemical and biological weapons.

"Partners in Progress." Fire Chief. August 2002.
http://firechief.com/ar/firefighting_partners_progress/index.htm. [2002-OCT-30]
Six city managers discuss their relationship with the fire department.

"Pascal's New Wager: The Dirty Bomb Threat." Center for Defense Information (CDI). http://www.cdi.org/terrorism/dirty-bomb.cfm. [2002-OCT-01]
Information on dirty bombs.

"Preparing for Terrorism: What Every Manager Needs to Know." International City/County Management Association (ICMA). http://www.icma.org/docs/500622.htm. [2002-OCT-30]
Steps city managers can take in evaluating and coordinating response to a terrorist threat.

"Public Health Emergency Preparedness and Response." Center for Disease Control and Prevention. http://www.bt.cdc.gov/. [2002-OCT-25]
Portal site for bioterrorism.

Public Safety Wireless Network Program. http://www.pswn.gov. [2002-OCT-30]
Information regarding public safety communications interoperability and wireless communications systems planning and implementation

"Radiation Studies – Emergency Response." CDC. National Center for Environmental Health. http://www.cdc.gov/nceh/radiation/response.htm. [2002-OCT-01]
Links to emergency response fact sheets, info about various types of radiation emergencies including nuclear attacks and dirty bombs.

"Regional Emergency Coordination Plan." Metropolitan Washington Council of Governments. Support Function 2, "Communications Infrastructure."
http://www.mwcog.org/homeland_plan/RESF_download.htm. [2002-OCT-30]
Case example of Washington Metro area emergency communications compatibility.

"Regional Emergency Preparedness Contacts: Safeguarding the Nation's Communities." Alliance for Regional Stewardship. March 2002.
http://www.regionalstewardship.org/Documents/REPCSReport.pdf. [2002-OCT-30]
Report on state/regional emergency preparedness, training, and community collaboration. Provides numerous local government case examples.

"Responding First to Bioterrorism." The National Academies. http://www.nap.edu/shelves/first/. [2002-OCT-25]
Portal site for first-responder resources regarding bioterrorism.

"Smallpox Response Plan and Guidelines." CDC.
http://www.bt.cdc.gov/agent/smallpox/response-plan/index.asp. [2002-OCT-25]
Comprehensive prevention and response guidelines for local health officials and experts.

"Some See Panic as Main Effect of Dirty Bombs." New York Times (March 7, 2002)
http://www.nytimes.com/2002/03/07/politics/07NUKE.html. [2002-OCT-01]
Information on dirty bombs.

State and Local Domestic Preparedness Support Helpline. U.S. Dept of Justice.
http://www.ojp.usdoj.gov/odp/docs/helpline.htm [2002-OCT-30]

"State, Local and Private Sector Coordination." White House Office of Homeland Security. http://www.whitehouse.gov/deptofhomeland/sect7.html. [2002-OCT-30]
Describes how the new Dept. of Homeland security would strengthen interoperability.

"State Radiation Control Agencies." Conference of Radiation Control Program Directors, Inc. http://www.crcpd.org/map/map.asp. [2002-OCT-01]
Lists state-by-state radiation control contacts.

"Talking About Disaster."The American Red Cross. http://www.redcross.org/disaster/safety/guide.html. [2002-NOV-11]
Guidebook developed to assist anyone providing disaster safety information to the public.

"Terrorism and Emergency Preparedness: Local Government Bio Terror Links". *Public Technology, Inc*. http://pti.nw.dc.us/task_forces/emergency_management/index.html. [2002-OCT-25]
Contains many local bioterror links, provides case examples from municipal government websites.

"Terrorism: Questions and Answers – Cyberterrorism" Council on Foreign Relations. http://www.terrorismanswers.com/terrorism/cyberterrorism.html. [2002-NOV-01]
Frequently asked questions about cyberterrorism.

"Testimony before the Special Oversight Panel on Terrorism." Denning, Dorothy. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. [2002-NOV-01]
Testimony of Dening, a Georgetown University Professor/Cyberterrorism expert, before a special congressional committee.

"Top 10 Suggestions from State Health Officials Who've Been There." National Governors Association. http://www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_3053,00.html. [2002-OCT-25]
Straightforward suggestions on what steps local health officials should take to prepare for a bioterrorism incident.

"ToxFAQ's– Frequently Asked Questions about Contaminants Found at Hazardous Waste Sites." Agency for Toxic Substances and Disease Registry. http://www.atsdr.cdc.gov/toxfaq.html. [2002-OCT-25]
List of hazardous chemicals and their effects.

"Trends in State Terrorism Preparedness." National Emergency Management Association. http://www.nemaweb.org/Trends_in_Terrorism_Preparedness/index.htm. [2002-OCT-30]
Report on state departments of homeland security and their overall effect on preparedness and capabilities.

"Tulsa Gears Up for Bioterrorism." National Journal. 14 Sept 02, pp. 2613-14. Local example of bioterrorism preparedness.

U.S. Army Chemical School 573-563-7257 http://www.wood.army.mil/usacmls/ [2002-NOV-18]

U.S. Army Medical Research Institute of Chemical Defense (MRICD) 410-671-2230 http://chemdef.apgea.army.mil/ [2002-NOV-18]

U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) 301-447-1333 http://www.usamriid.army.mil/education/index.html [2002-NOV-18]

U.S. Army Office of the Surgeon General (OTSG) (USAMRIID) 301-619-4535http://hld.sbccom.army.mil/ps/ps_wmd_ip.htm [2002-NOV-18]

U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section. http://www.cybercrime.gov/. [2002-NOV-01]
Investigative wing of the Dept. of Justice on computer crime.

University of the Health Sciences (USUHS) 301-295-0316 http://rad.usuhs.mil/ [2002-NOV-18]
"Weapons of Mass Destruction Training Program." Department of Justice – Office of Domestic Preparedness." http://www.ojp.usdoj.gov/odp/docs/coursecatalog.pdf. [2002-OCT-25]
Course catalog for all Department of Justice Training Programs, including chemical, biological, and other mass-destruction attacks.

"What is Cyber-terrorism?" SANS Institute. http://rr.sans.org/infowar/cyberterrorism.php. [2002-NOV-01]
Overview of the cyberterrorism threat with an extensive list of resources and web links.