Integrating Manmade Hazards into Mitigation Planning

Course No: F05-003

Credit: 5 PDH

Gilbert Gedeon, P.E.

Continuing Education and Development, Inc.
22 Stonewall Court
Woodcliff Lake, NJ 07677

P: (877) 322-5800
info@cedengineering.com

STATE AND LOCAL MITIGATION PLANNING
how-to guide

Integrating Manmade Hazards Into Mitigation Planning

Contents

the hazard mitigation planning process

Hazard mitigation planning is the process of determining how to reduce or eliminate the loss of life and property damage resulting from natural and manmade hazards. This diagram shows the four basic phases of the hazard mitigation process.

For illustration purposes, this diagram portrays a process that appears to proceed sequentially. However, the mitigation planning process is rarely linear. It is not unusual that ideas developed while assessing risks should need revision and additional information while developing the mitigation plan, or that implementing the plan may result in new goals or additional risk assessment.

organize resources

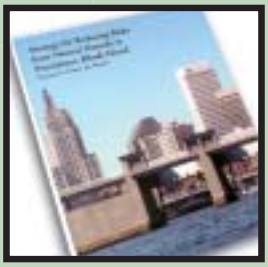
From the start, communities should focus on the resources needed for a successful mitigation planning process. Essential steps include identifying and organizing interested members of the community as well as the technical expertise required during the planning process.

assess risks

Next, communities need to identify the characteristics and potential consequences of hazards. It is important to understand how much of the community can be affected by specific hazards and what the impacts would be on important community assets.

develop a mitigation plan

Armed with an understanding of the risks posed by hazards, communities need to determine what their priorities should be and then look at possible ways to avoid or minimize the undesired effects. The result is a hazard mitigation plan and strategy for implementation.



implement the plan and monitor progress

Communities can bring the plan to life in a variety of ways ranging from implementing specific mitigation projects to changes in the day-to-day operation of the local government. To ensure the success of an ongoing program, it is critical that the plan remains relevant. Thus, it is important to conduct periodic evaluations and make revisions as needed.

foreword

foreword

The Federal Emergency Management Agency (FEMA) has developed this series of mitigation planning "how-to" guides to assist states, communities, and tribes in enhancing their hazard mitigation planning capabilities.

mit-i-gate\ 1: to cause to become less harsh or hostile; **2:** to make less severe or painful

plan-ning\ : the act or process of making or carrying out plans; *specif:* the establishment of goals, policies and procedures for a social or economic unit

These guides are designed to provide the type of information state and local governments need to initiate and maintain a planning process that will result in safer communities. These guides are applicable to states and communities of various sizes and varying ranges of financial and technical resources.

This how-to series is not intended to be the last word on any of the subject matter covered; rather, it is meant to provide clear guidance for the field practitioner. In practice, these guides may be supplemented with more extensive technical resources and the use of experts when necessary.

The series consists of four guides covering the core aspects of the planning process, and additional guides addressing special topics in hazard mitigation. The "core four" guides cover:

- Getting started with the mitigation planning process, including important considerations for how you can organize your efforts to develop an effective mitigation plan (FEMA 386-1);
- Identifying hazards and assessing losses to your community or state (FEMA 386-2);
- Setting mitigation priorities and goals for your community or state and writing the plan (FEMA 386-3); and
- Implementing the mitigation plan, including project funding and maintaining a dynamic plan that changes to meet new developments (FEMA 386-4).

Special topics covered include:

- Evaluating potential mitigation actions through the use of benefit-cost analysis and other techniques (FEMA 386-5);

- Incorporating special considerations into hazard mitigation planning for historic properties and cultural resources (FEMA 386-6);
- Incorporating mitigation considerations for manmade hazards into hazard mitigation planning, the topic of this how-to guide (FEMA 386-7);
- Using multi-jurisdictional approaches to mitigation planning (FEMA 386-8); and
- Finding and securing technical and financial resources for mitigation planning (FEMA 386-9).

Why should you take the time to read these guides?

- It simply costs too much to address the effects of disasters only after they happen;
- State and federal aid is usually insufficient to cover the full extent of physical and economic damages resulting from disasters;
- You can prevent a surprising amount of disaster damage if you understand where and how these phenomena occur;
- You can lessen the impact of both natural and technological hazards and speed the response and recovery process; and
- The most meaningful steps in avoiding the impacts of hazards are taken at the state and local levels by officials and community members who have a personal stake in the outcome and/or the ability to follow through on a sustained program of planning and implementation.

The guides focus on showing how mitigation planning:

- Can help your community become more *sustainable and disaster-resistant* through selecting the most appropriate mitigation actions, based on the knowledge you gain in the hazard identification and risk assessment process;
- Allows you to *focus your efforts on the hazard areas most important to you* by determining and setting priorities for mitigation planning efforts; and

- Can *save you money* by providing a forum for engaging in partnerships that could provide technical, financial, and/or staff resources in your effort to reduce the effects, and hence the costs, of natural and manmade hazards.

These guides provide a range of approaches to preparing a hazard mitigation plan. There is no one right planning process. However, there are several elements that are common to all successful planning endeavors, such as engaging citizens, developing goals and objectives, and monitoring progress. Select the approach that works best in your state or community.

This special-topic guide, *Integrating Manmade Hazards Into Mitigation Planning*, is not designed to help you establish procedures to respond to disasters, write an emergency operations plan, or create a counter-terrorism program for your community; rather, it assumes that your community is engaged in the mitigation planning process and serves as a resource to help you expand the scope of your plan to address terrorism and technological hazards. It provides information to supplement your community's hazard mitigation planning efforts. Because each of the four mitigation planning phases is covered comprehensively in its own how-to guide, references to other publications in the series are often used in lieu of full explanations of a process or activity. Furthermore, the guide is intended not as a highly technical manual but rather as a source of general guidance for the broad audiences that are likely to comprise state and local mitigation planning teams, including participants from government agencies, community interest groups, industrial partners, and others.

introduction

introduction

Disasters are events that can cause loss of life and property, environmental damage, and disruption of governmental, social, and economic activities. They occur when hazards impact human settlements and the built environment. Throughout the Cold War, the focus of emergency management planning was on responding to and recovering from nuclear attack by foreign enemies. During the 1990s, this emphasis shifted to address natural disasters such as hurricanes, earthquakes, tornadoes, and floods.

Yet again, the need to incorporate new threats into emergency management planning—this time, manmade hazards such as terrorism and technological disasters—has become all too apparent, as demonstrated by the September 11, 2001 attacks on New York City and Washington, DC and the July 2001 hazardous material train derailment and fire in Baltimore, Maryland. Additionally, the 2001 anthrax attacks, the 1996 bombing at the summer Olympics in Atlanta, the 1995 destruction of the Murrah Federal Building in Oklahoma City, the 1993 World Trade Center bombing, and scores of smaller-scale incidents and accidents reinforce the need for communities to reduce their vulnerability to future terrorist acts and technological disasters.

Manmade Hazards

For the purpose of this guide, "manmade hazards" are **technological hazards** and **terrorism.** These are distinct from natural hazards primarily in that they originate from human activity. In contrast, while the risks presented by natural hazards may be increased or decreased as a result of human activity, they are not inherently human-induced.

The term **"technological hazards"** refers to the origins of incidents that can arise from human activities such as the manufacture, transportation, storage, and use of hazardous materials. For the sake of simplicity, this guide assumes that technological emergencies are accidental and that their consequences are unintended.

The term **"terrorism"** refers to intentional, criminal, malicious acts. There is no single, universally accepted definition of terrorism, and it can be interpreted in many ways. Officially, terrorism is defined in the *Code of Federal Regulations* as "...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 CFR, Section 0.85). The Federal Bureau of Investigation (FBI) further characterizes terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorist organization; however, the origin of the terrorist or person causing the hazard is far less relevant to mitigation planning than the hazard itself and its consequences.

For the purposes of this guide, "terrorism" refers to the use of Weapons of Mass Destruction (WMD), including biological, chemical, nuclear, and radiological weapons; arson, incendiary, explosive, and armed attacks; industrial sabotage and intentional hazardous materials releases; and "cyber-terrorism." Within these general categories, however, there are many variations. Particularly in the area of biological and chemical weapons, there are a wide variety of agents and ways for them to be disseminated.

Although this series of mitigation planning how-to guides—as well as mitigation planning mandates such as the Disaster Mitigation Act of 2000 (DMA 2000)—grew out of a focus on planning for natural hazards, recent events suggest that an all-hazard mitigation plan should also address hazards generated by human activities such as terrorism and hazardous material accidents. While the term "mitigation" refers generally to activities that reduce loss of life and property by eliminating or reducing the effects of disasters, in the terrorism context it is often interpreted to include a wide variety of preparedness and response actions. For the purposes of this how-to guide, the traditional meaning will be assumed; that is, "mitigation" refers to specific actions that can be taken to reduce loss of life and property from manmade hazards by modifying the built environment to reduce the risk and potential consequences of these hazards.

To better structure the way in which we manage disasters, the concept of the "four phases of emergency management" was introduced in the early 1980s after the similarities between natural disaster preparedness and civil defense became clear. This approach can be applied to all disasters.

- *Mitigation* is defined as any sustained action taken to reduce or eliminate long-term risk to life and property from a hazard event. Mitigation, also known as prevention (when done before a disaster), encourages long-term reduction of hazard vulnerability. The goal of mitigation is to decrease the need for response as opposed to simply increasing the response capability. Mitigation can save lives and reduce property damage, and should be cost-effective and environmentally sound. This, in turn, can reduce the enormous cost of disasters to property owners and all levels of government. In addition, mitigation can protect critical community facilities, reduce exposure to liability, and minimize community disruption.
- *Preparedness* includes plans and preparations made to save lives and property and to facilitate response operations.
- *Response* includes actions taken to provide emergency assistance, save lives, minimize property damage, and speed recovery immediately following a disaster.
- *Recovery* includes actions taken to return to a normal or improved operating condition following a disaster.

FEMA developed the Integrated Emergency Management System (IEMS) using an all-hazards approach. While the IEMS was established as an "all-hazard" approach, responding to the threat of terrorism (referred to as *counter*terrorism) came to be viewed as the responsibility of law enforcement, defense, and intelligence agencies. Furthermore, defensive efforts to protect people and facilities from terrorism (referred to as *anti*terrorism) were generally limited to the government sector, the military, and some industrial interests. However, both technological disasters and incidents of domestic and international terrorism on United States soil during the past decade have made it clear that emergency managers, first responders, and planners must now work together to build better and safer communities in the 21st century.

While you may not be able to prevent every accident or deliberate attack, it is well within your ability to reduce the likelihood and/or the potential effects of an incident through mitigation. The process of mitigating hazards before they become disasters is similar for both natural and manmade hazards. Whether you are dealing with natural disasters, threats of terrorism, or hazardous materials accidents, you will use a process of 1) identifying and organizing your resources; 2) conducting a risk or threat assessment and estimating potential losses; 3) identifying mitigation actions that will reduce the effects of the hazards and creating a strategy to place them in priority order; and 4) implementing the actions, evaluating the results, and keeping the plan up-to-date. This four-phase process is known as mitigation planning.

In one form or another, planning is an element of almost everything that individuals, institutions, corporations, and governments do. Planning helps to coordinate actions, determine the order in which goals are accomplished, leverage opportunities, and identify priorities for allocating resources. Hazard mitigation planning is the integration of these activities into a community's emergency management programs in order to reduce or eliminate losses of life and property due to disasters.

The terms counterterrorism and antiterrorism are often used interchangeably. When using these terms, you should be careful to distinguish their meaning. *Counter*terrorism deals with offensively managing the threat of terrorism, while *anti*terrorism refers to defensive efforts to protect people and property.

Hazard Mitigation Planning

The hazard mitigation planning process consists of four basic phases as shown below. The first phase, Organize Resources, addresses the creation of a planning team with representatives from the public and private sectors, citizen groups, higher education institutions, and non-profits. The second phase, Assess Risks, explains identifying hazards and assessing losses. The third and fourth phases, Develop a Mitigation Plan and Implement the Plan and Monitor Progress, discuss establishing goals and priorities and selecting mitigation projects, and writing, implementing, and revisiting the mitigation plan, respectively.

How do you use this and the other how-to guides?

Integrating Manmade Hazards into Mitigation Planning, the seventh guide in the how-to series, provides information that will help you incorporate manmade hazards into the four phases of the mitigation planning process in your community or state, from organizing your resources to updating your plan. This how-to guide follows the four-phase mitigation process. Each section corresponds to one of the phases.

The planning process is as individual as the jurisdiction that engages in it. Each community or state approaches growth and change in a unique way, and the process of planning for the future should fit your particular community's or state's "personality." As a result, you should not consider the step-by-step sequence included in this and other how-to guides to be the only way to pursue mitigation planning. However, the process illustrated here is based on certain steps common to successful planning.

Types of Information Found in the How-to Series

The how-to series contains several types of information. Some information is highlighted with icons. Additional information can be found in Appendix C, Library.

Icons

The **"States"** icon identifies guidance focused solely on the role of the state. Although much of the information will be the same for local, tribal, and state governments, there are different requirements for state and local mitigation plans. Furthermore, states have additional responsibilities to assist local entities in their planning efforts. Guidance focusing on local governments applies to tribes as well.

The **"Caution"** icon alerts you to important information and ways to avoid sticky situations later in the planning process.

The **"DMA"** icon provides information relating to the mitigation planning requirements outlined in the Disaster Mitigation Act of 2000 (DMA 2000) regulations.

The **"Glossary"** icon identifies terms and concepts for which a detailed explanation is provided in Appendix B, Glossary.

The **"Tips"** icon identifies helpful hints and useful information that can be used in the planning process.

Library

A mitigation planning **"Library"** has been included in Appendix C. The library has a wealth of information, including Web addresses, reference sources, and other information. All of the Web sites and references listed in the how-to guide are included in the library.

Worksheets

Finally, to help track your progress, worksheets have been developed to correspond with the activities in this guide. These are included at the end of each section, where applicable, and in Appendix D, Worksheets. You can duplicate these forms and use them to organize your work as you implement the mitigation planning process.

phase 1


organize resources
assess risks
develop a mitigation plan
implement the plan and monitor progress

1 organize resources

Overview

Phase 1, *Organize Resources*, involves getting started in the hazard mitigation planning process by identifying and pulling together resources such as funding, staff, and political support. These resources will be necessary both to get the process off the ground and to achieve maximum effectiveness in the long term.

This section supplements the guidance provided in the *Getting Started: Building Support for Mitigation Planning* how-to guide (FEMA 386-1). Step 1 involves establishing community support for integrating manmade hazards into the mitigation planning process. Step 2 includes developing a list of stakeholders with expertise in hazardous materials, security issues, and law enforcement, among other disciplines, that you may want to add to your planning team. Step 3 discusses special considerations relevant to public participation activities.

Step 1
Assess Community Support

To be successful, a mitigation planning initiative requires the support of public officials, agency personnel, business owners and operators, citizens, and other community members. *Getting Started* discusses defining the planning area; gauging how much the community knows about mitigation planning; educating public officials on the hazards and risks in your community; using existing plans as a base from which to start; and organizing funding, technical, and human resources.

Inform the Public

One of the fundamental differences in planning for manmade disasters versus natural disasters is that most people have had little or no firsthand exposure to them. Even in light of the alarming increase in terrorist activity directed against the United States, the aging infrastructure, the persistence of security shortfalls in some sectors, and the proximity of industrial hazards to population centers, the public's perception of risk varies widely. This percep-

Planners should recognize that addressing manmade hazards may require that more attention be paid to dealing with a range of potentially strong personal responses, and they should be prepared to address potential concerns that may not have arisen during natural hazards planning such as security, unknown risks, and civil liberties. Thus, it is critical that planners develop a realistic, comprehensive picture of the hazards present in their communities to better educate the public and be prepared to respond to their concerns.

tion is influenced by many factors, such as media portrayal of events, the level of public education available, and an individual's experience with various hazards. Because the United States has a relatively short history of dealing with manmade hazards, discussions on this subject may be characterized by elements of uncertainty and even fear. Therefore, to gain public support, it is important to educate public officials, citizens, and the private sector about the manmade hazards that may affect the community and about the prevention and mitigation actions that can help address them. The planning team must present a realistic assessment of the potential consequences of such disasters while taking care to avoid overstating or inflating the risk.

Promote the Benefits of Mitigation Planning

Summary of the benefits of mitigation planning

- Reduces future losses from disasters
- Builds partnerships
- Facilitates funding priorities
- Contributes to sustainable communities

You can further educate people and build support by emphasizing the value added by mitigation planning and building on planning opportunities that already exist. Although manmade hazards may not be as easy to identify and predict as some natural hazards, the benefits of planning for such events are the same: improved disaster resistance, community involvement in the process, partnerships with sectors you may not have interacted with before, and more sustainable communities. Building on existing opportunities is a good way to create momentum for mitigation planning.

Many people are concerned about manmade hazards since the attacks of 2001, and the media have focused intensely on these disasters. You can use this high visibility to show why your community should plan for such contingencies. *Getting Started* examines ways to implement natural hazard mitigation planning through existing plans; now you can reexamine those plans with a focus on how to integrate planning for manmade disasters into them.

You may want to point out the following benefits as you educate others:

1. Mitigation helps local, tribal, and state governments fulfill their responsibility to protect their citizens, property, and environment by reducing the potential impacts of manmade disasters.
2. Mitigation can enhance a community's ability to recover from the impacts of a manmade disaster.
3. Mitigation can reduce exposure to civil or criminal liability in the event of a terrorist attack or technological accident.

Depending on the nature of the incident, the impacts of a manmade hazard can be localized—even limited to a single building—or they can be widespread, encompassing a metropolitan area, a watershed, or a transportation corridor. Additionally, the extent of the physical damages generated by an incident can be surpassed by its associated economic impacts, as demonstrated by the national-level economic effects of the September 11, 2001 attacks.

4. Mitigation actions may help reduce insurance premiums.

Capitalize on Planning Opportunities

As mentioned previously, manmade hazards can be integrated into existing planning efforts. The following opportunities should be considered:

1. **Planning during post-disaster recovery.** Following the September 2001 attacks, the increased risk of manmade hazards became a topic of conversation in the mainstream media and across the nation. This widespread interest can serve as an impetus to enhance a mitigation plan with actions that can reduce the effects of future attacks.

DMA

The Disaster Mitigation Act of 2000 provides an impetus for state and local governments to undertake mitigation planning. The Act does not mandate that terrorism or technological disasters be addressed in hazard mitigation planning; however, it does encourage and reward state and local pre-disaster planning and promote sustainability as a strategy for reducing the effects of disasters. Naturally, this objective can only be fully achieved through incorporating not only natural hazards but also the full spectrum of manmade disasters. Interim final regulations on hazard mitigation planning were published in the Federal Register on February 26, 2002 (see 44 CFR Parts 201 and 206).

2. **Comprehensive and other community-oriented planning activities**. If your community has begun developing or updating its comprehensive plan, capital improvement plan, urban design guidelines, land development regulations, growth management or sustainability plans, or other community-oriented guidance, this is a prime opportunity to incorporate planning for manmade disasters. For example, if your community is planning to build a new city hall or hospital, you can incorporate defensive architecture, site planning, and design approaches into the facility planning process to reduce the hazards to the facility from manmade events.

Planners are encouraged to link together as many planning opportunities as possible to maximize coordination, thoroughness, information sharing, and cost-effectiveness. Relevant planning actions may be ongoing or may already have been accomplished in your jurisdiction as part of other emergency management planning initiatives. For example, some jurisdictions completed a community vulnerability assessment as part of the Department of Justice's State Domestic Preparedness Support Program (equipment grant program – now within DHS); this information is directly transferable from first responder planning to mitigation planning.

At the time of this writing, the long-term consequences of the insurance industry's response to the events of September 11, 2001 are not clear. To date, the industry is having difficulty estimating the frequency and magnitude of future terrorism risks and is concerned about ensuring adequate capital to absorb the potential costs of another catastrophic attack. As a result, many insurers are establishing coverage limitations and raising premiums and deductibles for commercial customers. Risk is being shifted from insurers to property owners and business operators, and future attacks may lead to greater direct losses to those impacted—further emphasizing the importance of taking actions to reduce vulnerability and minimize losses.

(Source: General Accounting Office, *Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities*)

The results of the Institute for Business & Home Safety's 2001 study *Are We Planning Safer Communities? Results of a National Survey of Community Planners and Natural Disasters* show that the safest communities are located in states where hazards are a required consideration in comprehensive planning. In many states, however, this "best practice" is not followed. Ideally, hazard considerations are an integral part of state and local comprehensive planning; if they are not, state and local governments should consider requiring that comprehensive planning include all-hazard considerations.

3. **Update of existing mitigation plans or other emergency management plans**. In order to keep plans up-to-date, state and local governments must perform periodic reviews of existing plans. During these reviews, planners should re-evaluate the hazards that can affect their communities and update their plans as appropriate to incorporate manmade hazards.

Step 2
Build the Planning Team

Assuming you have already set up your planning team, expanding its scope to incorporate terrorism and technological disasters will require enhancing the team's capabilities by acquiring expertise in a number of disciplines. To ensure that the composition of the mitigation planning team contains the right mix of members, the capabilities of the existing team should be assessed and any gaps filled. To prevent the team from becoming so large as to be unwieldy, a committee/subcommittee approach may be implemented. You may wish to use the categories listed below to define the various subgroup areas of the planning team.

The size and composition of the planning team will depend on the community or state, size of the planning area, planning needs, and resources available. A team approach is optimal because:

a. It encourages participation and gets more people invested in the process

b. It enhances the visibility and stature of the planning process

c. It provides for a broad perspective on the issues

d. It provides the widest possible range of expertise and experience

e. It ensures the use of resources in a coordinated fashion to maximize benefits

Getting Started: Building Support for Mitigation Planning (FEMA 386-1) outlines methods for identifying stakeholders for a natural hazard mitigation planning process. Existing groups, such as natural hazard mitigation planning teams or emergency planning committees, can serve as ideal bases for manmade hazard mitigation efforts. Such teams should have a broad-based membership that includes, at a minimum, representatives of elected officials, emergency management, first responder agencies, healthcare, local environmental and transportation groups, the media, community groups, and representative owners and operators of private facilities.

A community's hazard mitigation planners are its primary resource for leading and coordinating efforts to reduce vulnerabilities in the built environment. In any given community, however, there may be a variety of other entities operating to the same end, either in concert with mitigation planning or independently. These may comprise public, private, or partnered initiatives; they may cut across local, state, and/or federal jurisdictions; and they may address planning, security, safety, engineering, and other aspects of hazard reduction. While projects such as these are often undertaken in a vacuum—that is, without relation to the community as a whole—their key personnel may possess or have access to expertise and resources that will enhance the ability of the hazard mitigation planning team to meet the state's or community's goals. The importance of thinking inclusively and holistically when recruiting team members becomes especially clear when planners are confronted with new and generally unfamiliar challenges such as integrating manmade hazards into mitigation planning.

Expertise that will be helpful in addressing manmade hazards may be lacking from a purely natural-hazards oriented team. Such expertise includes the following:

- Chemical emergency planning
- Counter- and antiterrorism (law enforcement and military)
- Crime prevention planning, including situational crime prevention and Crime Prevention Through Environmental Design (CPTED)
- Electrical engineering
- Emergency management
- Explosives/blast characteristics
- Fire protection engineering
- Force protection (protection of military personnel and facilities)
- Industrial security
- Mechanical engineering, including heating, ventilation, and air conditioning (HVAC)
- Protective/defensive architecture
- Site planning, urban design, and landscape design
- Structural engineering, design, and construction

Although situational crime prevention and Crime Prevention Through Environmental Design (CPTED) are closely related, the two are not synonymous. Situational crime prevention encompasses many CPTED principles but focuses more on managerial and user behavior factors that affect opportunities for criminal behavior in the specific setting for the specific crime(s) being addressed. CPTED, on the other hand, focuses more on changing the physical design aspects of environments to deter criminal activity.

Specialized expertise in these fields can be found at a number of sources, even in communities with modest resources. Additionally, technical assistance from the federal government may be available to communities. Among the many federal organizations offering relevant support are the Department of Homeland Security (DHS), the Environmental Protection Agency (EPA), and the Department of Justice (DOJ). See Appendix C for Web links to these agencies' programs.

See **Worksheet #1: Build the Planning Team** at the end of this section (also included in Appendix D) to help you identify additional team members.

The planning team should work with elected officials to formalize the community's commitment to planning and to promote an atmosphere of cooperation by "authorizing" the planning team to take the steps necessary to develop a mitigation plan for terrorism and technological hazards. At a minimum, this authority can be established through a resolution or proclamation recognizing the team as an authorized agent of the community.

Step 3
Engage the Public

Given the dramatic nature of terrorism and technological hazards, the community will expect to be involved in and informed about the mitigation planning process. *Getting Started* discusses developing a schedule or program for involving the public throughout the mitigation planning process. Adding a manmade hazard element to your public participation program will simply be another step. Keep in mind, however, that care must be taken when presenting certain types of information.

Because citizens may be fearful or upset about recent events and apprehensive about publicized threats, they may want to engage public officials in talking about such issues. The planning team should encourage the public to focus on what they can realistically do to protect their community and limit the time spent discussing issues that are outside the scope of their influence. For example, they may be concerned about travel safety and would like to see changes in airport security, but federal government agencies control these issues—not the local planning team. To alleviate concerns about issues the community has no authority over, the planning team should be informed enough to provide an overview of who the various authorities are and what their responsibilities are for addressing manmade hazards. Including as many stakeholders as possible in the planning process can help turn these concerns into productive considerations and enhance rather than hinder the process.

Planners should note that some issues involved with technological hazards, such as industrial siting, hazardous materials transportation, or chemical storage and processing techniques, may be contentious and can cause friction among citizens, industry leaders, emergency planners, and other decision makers. Local Emergency Planning Committees (LEPCs) will likely already be involved with these issues and should be able to provide insight into how they can be addressed.

There are several stages in the mitigation planning process at which you can inform the public about your efforts to bring manmade hazards into your program. These stages are:

Hazard Identification and Risk Assessment. The planning team should inform the community of the complete spectrum of natural and manmade hazards it identifies and the risks they present, emphasizing that terrorism and technological disasters can strike not just in large cities, but in any community of any size. Although in some cases it will be necessary to limit the kinds of information shared, it is nevertheless important to provide the community with a realistic picture of the hazards and risks and to understand what the community considers to be an acceptable level of risk. It should be emphasized that while no amount of planning and mitigation can remove 100% of the risk from terrorism or technological emergencies, a thorough hazard identification process will help in

prioritizing the community's needs and allocating its resources effectively.

Mitigation Strategy Development. When developing a strategy for the hazard mitigation process, you should hold public meetings or workshops to discuss mitigation actions. The planning team should obtain public input into non-sensitive mitigation decisions, especially if the actions will have a long-term effect such as a change in traffic patterns or an increase in the surveillance of public places. The community should also have input into how to fund some mitigation actions, such as through taxes, bonds, loans, or grant programs. While citizens may be willing to pay for some actions, they may not be willing to support others.

Implementation and Monitoring of the Mitigation Plan. The planning team should keep the community informed of the implementation schedule and progress, although once again, it may be necessary to limit the kinds of information released to the public. The public should also be notified when the mitigation plan is reviewed and updated.

Once you have established community support, expanded the planning team to include manmade hazard experts, and engaged the public in the planning process, you will be ready to perform a hazard identification and risk assessment for your jurisdiction. Phase 2 will guide you through this process.

When addressing antiterrorism and other manmade hazard mitigation actions, you should recognize that many of these are sensitive and that information about them should be restricted to a very limited number of people. You must carefully consider whether each part of the process will be open to the public or whether for security reasons you will have only the planning team and perhaps a limited number of outside stakeholders (such as key public officials not on the planning team) discuss the best actions for certain critical facilities. See Phase 4 for sensitive information issues to consider.

Step 2 of Getting Started *(FEMA 386-1) discusses establishing a planning team with a broad range of backgrounds and experience represented. This worksheet suggests additional individuals, agencies, and organizations that should be included on a team to plan for manmade hazards. State organizations can be included on local teams when appropriate to serve as a source of information and to provide guidance and coordination.*

You should use the checklist as a starting point for expanding your team.

	ON TEAM	ADD TO TEAM
Specialists for Manmade Hazards		
Bomb and Arson Squads	☐	☐
Community Emergency Response Teams	☐	☐
Hazardous Materials Experts	☐	☐
Infrastructure Owners/Operators	☐	☐
National Guard Units	☐	☐
Representatives from facilities identified in Worksheet #2: Asset Identification Checklist	☐	☐
Local/Tribal		
Administrator/Manager's Office	☐	☐
Budget/Finance Office	☐	☐
Building Code Enforcement Office	☐	☐
City/County Attorney's Office	☐	☐
Economic Development Office	☐	☐
Emergency Preparedness Office	☐	☐
Fire and Rescue Department	☐	☐
Hospital Management	☐	☐
Local Emergency Planning Committee	☐	☐
Planning and Zoning Office	☐	☐
Police/Sheriff's Department	☐	☐
Public Works Department	☐	☐
Sanitation Department	☐	☐
School Board	☐	☐
Transportation Department	☐	☐
Tribal Leaders	☐	☐

	ON TEAM	ADD TO TEAM
Special Districts and Authorities		
Airport and Seaport Authorities	☐	☐
Business Improvement District(s)	☐	☐
Fire Control District	☐	☐
Flood Control District	☐	☐
Redevelopment Agencies	☐	☐
Regional/Metropolitan Planning Organization(s)	☐	☐
School Districts	☐	☐
Transit/Transportation Agencies	☐	☐
Others		
Architectural/Engineering/Planning Firms	☐	☐
Citizen Corps	☐	☐
Colleges/Universities	☐	☐
Land Developers	☐	☐
Major Employers/Businesses	☐	☐
Professional Associations	☐	☐
Retired Professionals	☐	☐
State		
Adjutant General's Office (National Guard)	☐	☐
Board of Education	☐	☐
Building Code Office	☐	☐
Climatologist	☐	☐
Earthquake Program Manager	☐	☐
Economic Development Office	☐	☐

	ON TEAM	ADD TO TEAM
Emergency Management Office/ State Hazard Mitigation Officer	☐	☐
Environmental Protection Office	☐	☐
Fire Marshal's Office	☐	☐
Geologist	☐	☐
Homeland Security Coordinator's Office	☐	☐
Housing Office	☐	☐
Hurricane Program Manager	☐	☐
Insurance Commissioner's Office	☐	☐
National Flood Insurance Program Coordinator	☐	☐
Natural Resources Office	☐	☐
Planning Agencies	☐	☐
Police	☐	☐
Public Health Office	☐	☐
Public Information Office	☐	☐
Tourism Department	☐	☐

Non-Governmental Organizations (NGOs)	ON TEAM	ADD TO TEAM
American Red Cross	☐	☐
Chamber of Commerce	☐	☐
Community/Faith-Based Organizations	☐	☐
Environmental Organizations	☐	☐
Homeowners Associations	☐	☐
Neighborhood Organizations	☐	☐
Private Development Agencies	☐	☐
Utility Companies	☐	☐
Other Appropriate NGOs	☐	☐

phase 2


organize resources
assess risks
develop a mitigation plan
implement the plan and monitor progress

2 assess risks

Overview

Phase 2 of the mitigation planning process, *Assess Risks*, involves identifying hazards and estimating potential losses. The results of these efforts will later be linked to estimates of the effectiveness of the mitigation projects you may be considering. There are some unique aspects to hazard characteristics, asset identification, and vulnerability assessment that will affect the way a risk assessment for terrorism and technological hazards is carried out. This how-to guide addresses these special considerations; please refer to *Understanding Your Risks: Identifying Hazards and Estimating Losses* (FEMA 386-2) for information on the more general aspects of the risk assessment process.

Step 1 Identify Hazards

The first step in any risk assessment is to identify the hazards that affect your community or state. Most manmade hazards fall into two general categories: terrorism (intentional acts) and technological hazards (accidental events). These two categories include the following hazards:

Terrorism

- Conventional bomb/improvised explosive device
- Biological agent
- Chemical agent
- Nuclear bomb
- Radiological agent
- Arson/incendiary attack
- Armed attack
- Cyberterrorism
- Agriterrorism
- Hazardous material release (intentional)

Research Existing Records, Plans, and Reports

Terrorist attacks and technological disasters occur infrequently enough in the United States that there may be few relevant records that can help determine what manmade hazards may affect the area being studied. Both the Federal Bureau of Investigation (FBI) and the U.S. Department of State (DOS) issue annual reports on terrorist activities domestically and around the world, and Local Emergency Planning Committees, State Emergency Response Commissions, and the United States Environmental Protection Agency are sources for historical data on hazardous material incidents throughout the U.S. Also, in many communities, plans are in place to respond to numerous types of technological hazards, and these plans—and the people who develop them—may be valuable sources of information about human-induced risks. In researching existing documentation, remember to consider information available from other levels of government whenever possible.

The following list identifies just a few of the documents that may be of use to the planning team:

- Existing mitigation plans
- Comprehensive plans
- Emergency operations plans
- Continuity of operations and other contingency plans
- Radiological emergency plans (nuclear power plants)
- Chemical stockpile emergency plans
- SARA Title III / hazardous material facility emergency plans
- Toxic Release Inventory Reports
- Statewide Domestic Preparedness Strategy

Technological Hazards

- Industrial accident (fixed facility)
- Industrial accident (transportation)
- Failure of Supervisory Control and Data Acquisition (SCADA) system or other critical infrastructure component

Within these various types of incidents, there are many variations, which illustrates one of the fundamental differences between natural and manmade hazards. The types, frequencies, and locations of many natural hazards are identifiable and even, in some cases, predictable. They are governed by the laws of physics and nature. Malevolence, incompetence, carelessness, and other behaviors, on the other hand, are functions of the human mind and, while they can be assumed to exist, they cannot be forecast with any accuracy. There is, therefore, the potential for most, if not all, types of manmade hazards to occur anywhere.

Your community or state's planning team should tap into available expertise in the areas listed earlier to develop a comprehensive list of the potential manmade hazards in your jurisdiction. You may also want to review reports and obtain briefings on the various plans government agencies and private companies have prepared in the event of an emergency. These may include radiological emergency plans, SARA Title III/hazardous material facility emergency plans, and chemical stockpile emergency plans, among others.

Weapons of Mass Destruction

Like terrorism itself, the term "Weapons of Mass Destruction" (WMD) has various definitions. Common to all of them is the assumption that WMDs comprise incendiary, explosive, chemical, biological, radioactive, and/or nuclear agents.

50 U.S.C., § 2302 defines WMD as follows:

"The term 'weapon of mass destruction' means any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of

(A) toxic or poisonous chemicals or their precursors;

(B) a disease organism; or

(C) radiation or radioactivity."

The United States Government *Interagency Domestic Terrorism Concept of Operations Plan* (CONPLAN) considers a WMD to be "any device, material, or substance used in a manner, in a quantity or type, or under circumstances evidencing an intent to cause death or serious injury to persons or significant damage to property."

One-Stop Shopping Resources for General Information on Manmade Hazards

http://www.fema.gov/hazards
(FEMA: links to authoritative sources of hazard information)

http://training.fema.gov/EMIWeb/terrorisminfor/ctrt.asp
(FEMA: terrorism-related training and resources)

While these information sources are primarily oriented toward emergency response, they can provide valuable insight to mitigation planners on how manmade hazards can impact communities.

Step 2
Profile Hazard Events

In the area of hazard profiling, there are significant differences between natural and manmade hazards, particularly those related to terrorism. Foremost among these is that terrorists have the ability to choose among targets and tactics, designing their attack to maximize the chances of achieving their objective. Similarly, accidents, system failures, and other mishaps are also largely unforeseeable. This makes it very difficult to identify how and where these hazards may occur. Notwithstanding the difficulty involved with predicting the occurrence of manmade disasters, the various consequences of these disasters are generally familiar to the sectors of the emergency planning and response community that already specialize in them: injuries and deaths, contamination of and/or damage to buildings and systems, and the like. Numerous authoritative sources exist that can provide detailed information on the nature of all of these hazards; however, more important for the purposes of hazard mitigation than details about the various agents' characteristics are the ways in which they can impact the built environment and what actions can be taken to reduce or eliminate the resulting damage.

Whether intentional or accidental, manmade disasters—as with natural disasters—involve the application of one or more modes of harmful force to the built environment. For the purposes of this how-to guide, these modes are defined as contamination (as in the case of chemical, biological, radiological, or nuclear hazards), energy (explosives, arson, and even electromagnetic waves), or failure or denial of service (sabotage, infrastructure breakdown, and transportation service disruption). The planning team should include expertise in these areas in order to develop a comprehensive list of the manmade hazards in your jurisdiction and identify the full spectrum of ways in which they might occur.

The following table, Event Profiles for Terrorism and Technological Hazards, is not intended to replace the expertise and knowledge of planning, security, or design professionals, but rather to help guide the planning team in understanding some of the ways in which these hazards can interact with the built environment. For each type of hazard, the following factors are addressed:

- *Application mode* describes the human act(s) or unintended event(s) necessary to cause the hazard to occur.
- *Duration* is the length of time the hazard is present on the target. For example, the duration of a tornado may be just minutes, but a chemical warfare agent such as mustard gas, if unremediated, can persist for days or weeks under the right conditions.
- The *dynamic/static characteristic* of a hazard describes its tendency, or that of its effects, to either expand, contract, or remain confined in time, magnitude, and space. For example, the physical destruction caused by an earthquake is generally confined to the place in which it occurs, and it does not usually get worse unless there are aftershocks or other cascading failures; in contrast, a cloud of chlorine gas leaking from a storage tank can change location by drifting with the wind and can diminish in danger by dissipating over time.
- *Mitigating conditions* are characteristics of the target and its physical environment that can reduce the effects of a hazard. For example, earthen berms can provide protection from bombs; exposure to sunlight can render some biological agents ineffective; and effective perimeter lighting and surveillance can minimize the likelihood of someone approaching a target unseen. In contrast, *exacerbating conditions* are characteristics that can enhance or magnify the effects of a hazard. For example, depressions or low areas in terrain can trap heavy vapors, and a proliferation of street furniture (trash receptacles, newspaper vending machines, mail boxes, etc.) can provide concealment opportunities for explosive devices.

The FBI's annual report *Terrorism in the United States* contains profiles and chronologies of terrorism incidents in America. The 1999 edition includes a comprehensive review of terrorist activities in the United States over the past three decades. This information is helpful to planners as data for hazard profiling; it also illustrates that manmade hazards impact not only large cities but commonly strike small to mid-sized communities as well—an important point when building public support for mitigating terrorism and technological hazards. The *Terrorism in the United States* reports can be downloaded from http://www.fbi.gov/publications/terror/terroris.htm.

Event Profiles for Terrorism and Technological Hazards

Hazard	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Conventional Bomb/ Improvised Explosive Device	Detonation of explosive device on or near target; delivery via person, vehicle, or projectile.	Instantaneous; additional "secondary devices" may be used, lengthening the time duration of the hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Overpressure at a given standoff is inversely proportional to the cube of the distance from the blast; thus, each additional increment of standoff provides progressively more protection. Terrain, forestation, structures, etc. can provide shielding by absorbing and/or deflecting energy and debris. Exacerbating conditions include ease of access to target; lack of barriers/shielding; poor construction; and ease of concealment of device.
Chemical Agent *	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/ containers; or munitions.	Chemical agents may pose viable threats for hours to weeks depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation of liquids. Humidity can enlarge aerosol particles, reducing inhalation hazard. Precipitation can dilute and disperse agents but can spread contamination. Wind can disperse vapors but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place can protect people and property from harmful effects.
Arson/ Incendiary Attack	Initiation of fire or explosion on or near target via direct contact or remotely via projectile.	Generally minutes to hours.	Extent of damage is determined by type and quantity of device/accelerant and materials present at or near target. Effects generally static other than cascading consequences, incremental structural failure, etc.	Mitigation factors include built-in fire detection and protection systems and fire-resistive construction techniques. Inadequate security can allow easy access to target, easy concealment of an incendiary device and undetected initiation of a fire. Non-compliance with fire and building codes as well as failure to maintain existing fire protection systems can substantially increase the effectiveness of a fire weapon.
Armed Attack	Tactical assault or sniping from remote location.	Generally minutes to days.	Varies based upon the perpetrators' intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons and undetected initiation of an attack.
Biological Agent *	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits and moving sprayers.	Biological agents may pose viable threats for hours to years depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate wind will disperse agents but higher winds can break up aerosol clouds; the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.

Event Profiles for Terrorism and Technological Hazards (continued)

Hazard	Application Mode	Hazard Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Cyber-terrorism	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.
Agriterrorism	Direct, generally covert contamination of food supplies or introduction of pests and/or disease agents to crops and livestock.	Days to months.	Varies by type of incident. Food contamination events may be limited to discrete distribution sites, whereas pests and diseases may spread widely. Generally no effects on built environment.	Inadequate security can facilitate adulteration of food and introduction of pests and disease agents to crops and livestock.
Radiological Agent **	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits and moving sprayers.	Contaminants may remain hazardous for seconds to years depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
Nuclear Bomb **	Detonation of nuclear device underground, at the surface, in the air or at high altitude.	Light/heat flash and blast/shock wave last for seconds; nuclear radiation and fallout hazards can persist for years. Electromagnetic pulse from a high-altitude detonation lasts for seconds and affects only unprotected electronic systems.	Initial light, heat and blast effects of a subsurface, ground or air burst are static and are determined by the device's characteristics and employment; fallout of radioactive contaminants may be dynamic, depending on meteorological conditions.	Harmful effects of radiation can be reduced by minimizing the time of exposure. Light, heat and blast energy decrease logarithmically as a function of distance from seat of blast. Terrain, forestation, structures, etc. can provide shielding by absorbing and/or deflecting radiation and radioactive contaminants.
Hazardous Material Release (fixed facility or trans-portation)	Solid, liquid and/or gaseous contaminants may be released from fixed or mobile containers.	Hours to days.	Chemicals may be corrosive or otherwise damaging over time. Explosion and/or fire may be subsequent. Contamination may be carried out of the incident area by persons, vehicles, water and wind.	As with chemical weapons, weather conditions will directly affect how the hazard develops. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place can protect people and property from harmful effects. Non-compliance with fire and building codes as well as failure to maintain existing fire protection and containment features can substantially increase the damage from a hazardous materials release.

* Source: *Jane's Chem-Bio Handbook*
** Source: FEMA, *Radiological Emergency Management* Independent Study Course

Step 3
Inventory Assets

As discussed in Step 1, the probability of manmade hazards occurring cannot be quantified with as great a level of accuracy as that of many natural hazards. Furthermore, these incidents generally occur at a specific location such as a building rather than encompassing a wide area such as a floodplain, and potential locations for terrorist attacks and technological disasters are likely to be distributed widely throughout your community. Thus, translating most manmade hazard profiles into meaningful geospatial information is difficult at best.

Instead, the planning team should use an asset-specific approach, identifying potentially at-risk critical facilities and systems in the community. Once a comprehensive list of assets has been developed, it should be prioritized so that the community's efforts can be directed to protect the most important assets first. Then, beginning with the highest priority assets, the vulnerabilities of each facility or system to each type of hazard should be assessed. A discussion of each of these steps follows.

The term "mitigation" in the context of this how-to guide refers to the physical aspects of vulnerability reduction. Thus, in identifying the areas of interest for the purposes of terrorism and technological hazards, planners should focus on specific places in their community where opportunities exist to reduce exposure to, and the potential consequences of, the various types of malevolent acts and accidental incidents that could occur. While this does require a highly facility-specific approach (e.g., the protection of a utility system, communications infrastructure, or government building), planners must be sure to consider the interconnectivity of all of the elements in the built environment such as buildings, infrastructures, and aggregations of human activity when determining the physical or geographic constraints of their planning activities.

Expand the Asset List

In expanding an existing asset list, the planning team should start by referring to the community's Emergency Operations Plan (EOP) to identify specific critical facilities, sites, systems, or other locations that could potentially be targeted for attack or that are at risk of being the site of an accident that could produce significant consequences. This process should take into account the dynamic nature of manmade events: while the physical consequences of some types of incidents generally remain localized (as with the bombing of a building), the impacts of others may spread well beyond the location of origin (as with a chlorine gas leak).

As part of the hazard mitigation planning process, you should develop a base map showing the assets in your jurisdiction. You can overlay this map with information representing manmade hazards and their potential consequences. Maps may not be able to actually predict where manmade hazards are most likely to strike, but they can help planners understand the interrelationships between assets and hazards. Through functions like buffering and dispersion modeling, planners can identify how proximity and clustering of assets may exacerbate the impacts of a particular type of attack, and even evaluate the implications of multiple vulnerabilities.

The initial inventory can be done very quickly and easily using the baseline data contained in HAZUS ("Hazards US"), FEMA's hazard loss estimation software that uses building stock, economic, geologic, and other data to provide loss estimates for earthquakes. You can identify medical care facilities; emergency response facilities; schools; dams; hazardous material sites; roads, airports, and other transportation facilities; electric power, oil, and gas lines; and other infrastructure. Refer to page 2-3 of *Understanding your Risks: Identifying Hazards and Estimating Losses* (FEMA 386-2) for help in creating a base map.

In addition to your EOP, **Worksheet #2: Asset Identification Checklist** at the end of this section (also included in Appendix D) is intended as an aid for identifying critical facilities, sites, systems, and other assets in your community or state. Step 3 provides some approaches for determining the importance of each asset to the community.

Critical Infrastructure Protection

Critical infrastructures are systems whose incapacity or destruction would have a debilitating effect on the defense or economic security of the nation. The critical infrastructure categories include:

Agriculture & food

Water

Public health

Emergency services

Defense industrial base

Telecommunications

Energy

Transportation

Banking & finance

Chemicals & hazardous materials

Postal & shipping

The President's Commission on Critical Infrastructure Protection (PCCIP) was established in July 1996 by Presidential Executive Order 13010 to formulate a comprehensive national strategy for protecting the infrastructures we all depend on from physical and "cyber" threats. The PCCIP included senior representatives from private industry, government, and academia, and was divided into five teams representing the critical infrastructures. Each team evaluated the growing risks, threats, and vulnerabilities within its sector. The sector teams and their industries included:

- *Information & Communications* – telecommunications, computers & software, Internet, satellites, fiber optics
- *Physical Distribution* – railroads, air traffic, maritime, intermodal, pipelines
- *Energy* – electrical power, natural gas, petroleum, production, distribution & storage
- *Banking & Finance* – financial transactions, stock & bond markets, federal reserve
- *Vital Human Services* – water, emergency services, government services

Threats to critical infrastructures can be posed by anyone with the capability, technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. Terrorists, insiders, disgruntled employees, and hackers are included in this profile. The fact that most of the nation's vital services are delivered by private companies creates a significant challenge in determining where the responsibility for protecting our critical infrastructures falls; the PCCIP addressed this challenge by bringing the private and public sectors together to assess infrastructure vulnerabilities and develop assurance strategies for the future, consulting with industry executives, security experts, government agencies, and private citizens. State and local mitigation planning teams are encouraged to draw on this model as a basis for their own efforts to incorporate terrorism and technological hazard mitigation into their planning processes.

Source: Critical Infrastructure Assurance Office at www.ciao.gov.

References and background information on critical infrastructure protection can be found on the Critical Infrastructure Assurance Office's web site at http://www.ciao.gov/resource/pccip/pccip_documents.htm.

Assess Vulnerabilities

The vulnerabilities of a given facility, site, system, or other asset can be identified based on two distinct but complementary approaches. First, any given place in the built environment has a certain level of *inherent vulnerability* that exists independent of any protective or mitigation actions that are applied to it. For example, a football stadium is a setting where thousands of people gather, and a terrorist may find

such a target very attractive in that many people would be hurt in an attack. An assessment of such inherent vulnerabilities must be conducted for each asset to determine its weaknesses. Second, the security, design, and other mitigation tools used to protect a place determine its *tactical vulnerability*. For example, if an HVAC system is designed so that its components are not visible to the public and has security cameras aimed at it, a terrorist may be less likely to attempt to use the system as a weapon to release poisonous gas. A tactical vulnerability assessment should be completed for each asset to determine how well it is protected from an attack.

Inherent Vulnerability. Using the asset inventory you assembled in Step 3, the planning team can assess the inherent vulnerability of each asset based on:

- *Visibility:* How aware is the public of the existence of the facility, site, system, or location?
- *Utility:* How valuable might the place be in meeting the objective(s) of a potential terrorist or saboteur?
- *Accessibility:* How accessible is the place to the public?
- *Asset mobility:* Is the asset's location fixed or mobile? If mobile, how often is it moved, relocated, or repositioned?
- *Presence of hazardous materials:* Are flammable, explosive, biological, chemical, and/or radiological materials present on site?
- *Potential for collateral damage:* What are the potential consequences for the surrounding area if the asset is attacked or damaged?
- *Occupancy:* What is the potential for mass casualties based on the maximum number of individuals on site at a given time?

Completing **Worksheet #3: Facility Inherent Vulnerability Assessment Matrix** at the end of this section (also included in Appendix D) will help you determine how vulnerable each asset is and how vulnerable the assets are relative to each other.

In conducting the vulnerability assessment, it is important to ensure that the focus is not only on hazard reduction but also includes preparedness, response, and recovery considerations. For example, allowing unrestricted vehicle access to a building may create some risk of a vehicle bomb attack, but it also helps ensure easy fire apparatus access for emergency response purposes. Thus, just as it is important to balance security and openness in planning and design, it is critical to consider the secondary hazards that could arise from well-intended efforts to reduce vulnerabilities.

Tactical Vulnerability. The following list will help the planning team assess the tactical vulnerability of the assets in the community. The tactical vulnerability of each asset is based on:

Site Perimeter

- *Site Planning and Landscape Design*: Is the facility designed with security in mind—both site-specific and with regard to adjacent land uses?
- *Parking Security*: Are vehicle access and parking managed in a way that separates vehicles and structures?

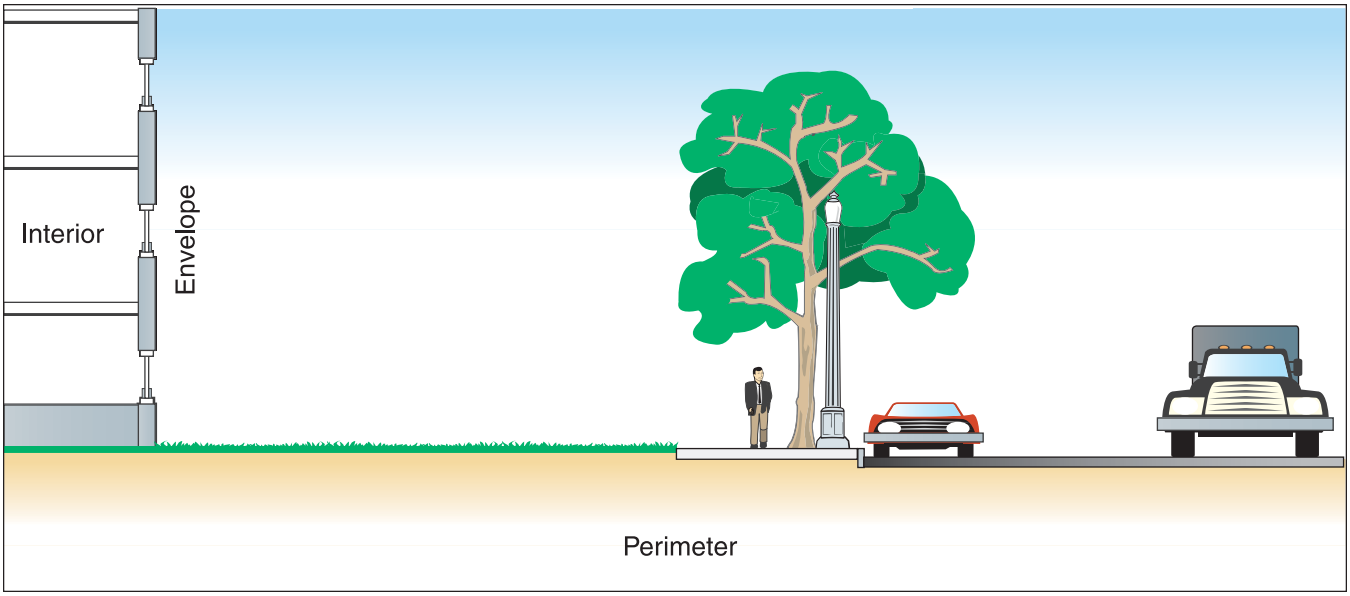
Building Envelope

- *Structural Engineering*: Is the building's envelope designed to be blast-resistant? Does it provide collective protection against chemical, biological, and radiological contaminants?

Facility Interior

- *Architectural and Interior Space Planning*: Does security screening cover all public and private areas? Are public and private activities separated? Are critical building systems and activities separated?
- *Mechanical Engineering*: Are utilities and HVAC systems protected and/or backed up with redundant systems?

Tactical Vulnerability Considerations



- *Electrical Engineering*: Are emergency power and telecommunications available? Are alarm systems operational? Is lighting sufficient?
- *Fire Protection Engineering*: Are the building's water supply and fire suppression systems adequate, code-compliant, and protected? Are on-site personnel trained appropriately? Are local first responders aware of the nature of the operations at the facility?
- *Electronic and Organized Security*: Are systems and personnel in place to monitor and protect the facility?

A list of mitigation actions that correspond to the factors described above can be found in Phase 3, *Develop a Mitigation Plan*, in this guide.

Establish Mitigation Priorities

For the purpose of developing a realistic prioritization of manmade hazard mitigation projects, three elements should be considered in concert: the relative importance of the various facilities and systems in the asset inventory, the vulnerabilities of those facilities, and the threats that are known to exist.

Asset criticality. The first element, asset criticality, is a measure of the importance of the facility or system to the community. Considerations in determining asset criticality include:

- Is it an element of one of the community's critical infrastructures?
- Does it play a key role in your community's government, economy, or culture?
- What are the consequences of destruction, failure, or loss of function of the asset in terms of fatalities and/or injuries, property losses, and economic impacts?
- What is the likelihood of cascading or subsequent consequences should the asset be destroyed or its function lost?

Vulnerability. The second factor was addressed in the previous section, Assess Vulnerabilities. By identifying the most exploitable weaknesses of each asset, the planning team can identify vulnerabilities in greatest need of attention. This, in effect, gives the planning team a criterion to use in establishing mitigation priorities so that the community can focus its efforts on addressing the most critical issues.

Prioritizing Mitigation Requirements: The General Services Administration Approach to Security Standards

The General Services Administration (GSA) is the United States government's landlord. As such, it is responsible for security at more than 1,000 federal facilities, both owned and leased. To meet this need, GSA uses a standards-based approach that involves assessing and categorizing facilities and assigning minimum security standards to each category.

Facility Security Levels

In order to determine the appropriate package of security measures for each facility, a five-level classification system is used to rate facilities based on **occupancy**, **size**, **level of public contact**, **type of operations**, and the **nature of the agencies** present in the facility.

You can adapt this model to help prioritize mitigation projects by establishing criteria based on the assets present in your community. In a small town, for example, a three-level system may be adequate: the City Hall complex, containing the offices of elected and administrative officials as well as Police Headquarters and an Emergency Operations Center, would qualify as a Level III facility; the city's maintenance yard might fall within Level II; and a remote sewage lift station would be assigned Level I status.

Recommended Minimum Security Standards

The GSA list of security standards can serve simply as a list of recommended measures; however, to better allocate resources, measures can be linked to facility security levels. For example, the most basic measures may be *mandated* for all facilities, while the most stringent or sophisticated measures may be *required* only for the highest level facilities, *recommended* for middle-level facilities, and *unnecessary* for the lowest-level facilities. The following criteria are among those considered for each category of security measures:

- Perimeter security – parking, closed-circuit television, lighting, physical barriers
- Entry security – receiving & shipping, access control, entrances & exits
- Interior security – employee & visitor identification, utilities, occupant emergency plan, day care centers
- Security planning – tenant assignment, construction & renovation (this category also includes intelligence-sharing, training, and administrative procedures, which are outside the scope of this guidance)

Source: U.S. Department of Justice, *Vulnerability Assessment of Federal Facilities*

Threat. The last element, threat, is fundamental to the prioritization process but very difficult to quantify. It answers the question "what must we mitigate against?" The frequency of a hazard's occurrence is an important factor in establishing mitigation priorities, but unfortunately it is impossible to determine with any precision in the case of terrorism (for technological hazards, "threat" can be interpreted to mean the likelihood of some type of human-induced unintentional event). Instead of being influenced by predictable, quantifiable natural forces, terrorism—and to some degree, other technological hazards—is the result of human behavior that often lies outside conventional ideals of appropriateness and rationality and is thus difficult to predict.

In understanding the threat of terrorism, historical data can be of some value in that it illustrates the types of tactics that have been used previously (and thus may be used again); however, the historical approach is far from definitive because, in addition to the fact that threat information lacks the predictive accuracy needed for making decisions of this type, the origin and nature of the threats constantly change with technology, political issues, and other factors that compel and enable terrorist activity. Further complicating the use of threat information in determining relative risk, once a protective action is applied to an asset and its vulnerability reduced relative to that of a comparable target, the balance of target attractiveness—and thus the likelihood of attack—may be altered, displacing some risk onto another asset that has become relatively more vulnerable.

The most useful application of threat information for mitigation planning purposes, then, will be as a guide to the types of incidents that are relatively most likely to occur. Clearly, the level of detail that can be provided to the planning team will be determined by the sensitivity of the threat information. The broadest threat estimates may be so vague as to be of little use, while the most current and specific information may be part of ongoing criminal and/or intelligence investigations and thus not available for mitigation planning purposes. However, it should be possible to obtain a useful level of understanding through consultation with local, state, and federal law enforcement agencies that can provide the planning

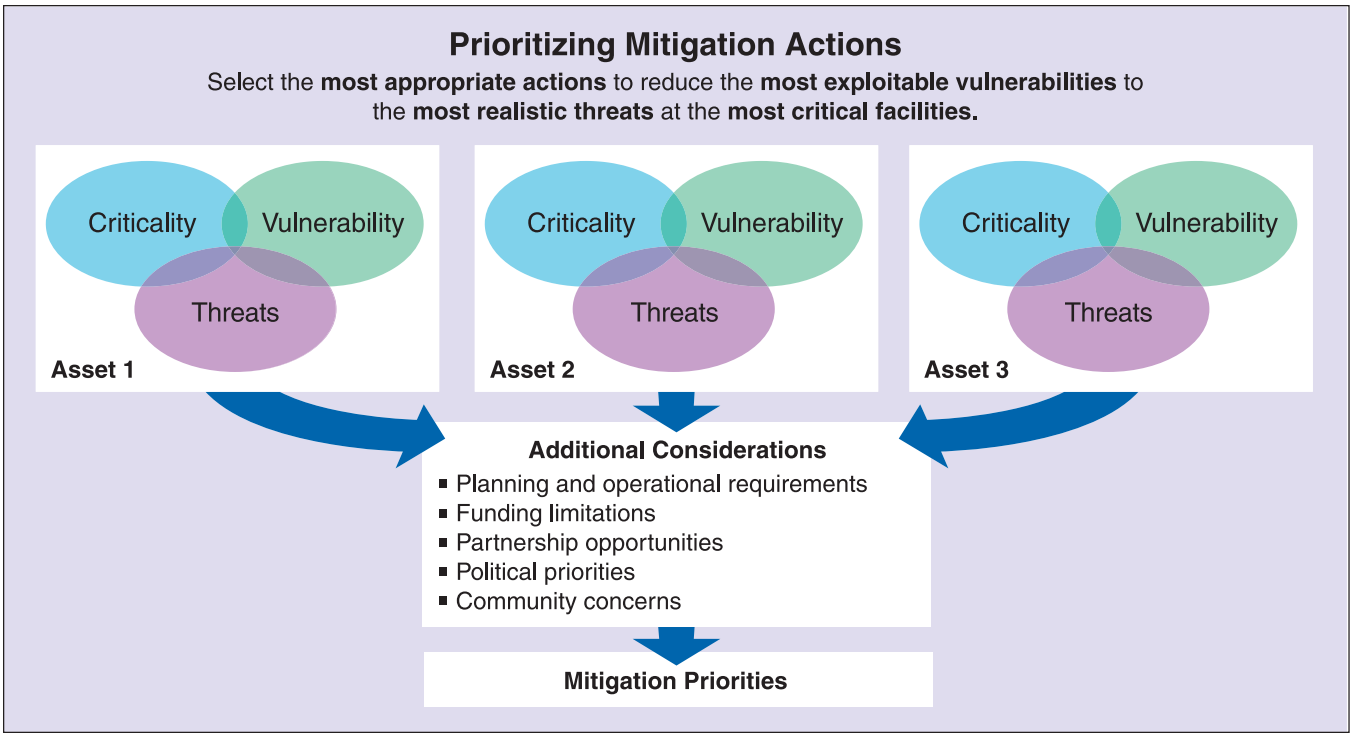
team with a general characterization of terrorist and other such groups known to be active in your community, the tactics they may employ or have employed in the past, and projections of potential and emerging threats.

In addition to asset criticality, vulnerability, and threat, the planning team may also take the following considerations into account when prioritizing projects:

- What assets were of concern during your community's Y2K planning?
- What assets support the continuity of your jurisdiction's governmental operations and essential functions?
- What assets support the implementation of your jurisdiction's EOP, Emergency Support Functions (ESFs), and Incident Command/Unified Command systems?
- What political priorities may be relevant?
- To what extent will funding constraints limit mitigation options?

The following diagram illustrates the prioritizing process.

The list you develop of the assets most important to protect will help you focus your loss estimation analysis in Step 4.



Step 4
Estimate Losses

As with natural hazard risk assessment processes, the potential losses from manmade hazards are generally grouped into three categories: *people* (death and injury), *assets* (structures and their contents), and *functions* (provision of services and generation of revenue). However, terrorism and technological disasters present some unique implications for loss estimation. As previously discussed, for example, the key issue of frequency of occurrence (also called "recurrence interval") is elusive in the case of manmade hazards because of the difficulties associated with predicting human behavior and with acquiring and applying appropriate threat data.

For some hazards, worst-case scenarios can be generated and losses estimated if the hazard can be characterized with some precision. CAMEO (Computer-Aided Management of Emergency Operations) software is one application that has been used extensively for preparedness and response activities relating to hazardous materials. For example, using the location of rail lines and the kinds and quantities of hazardous materials transported over them, models can be used to estimate the consequences of various chemical release scenarios. Particular attention can be paid to considerations such as evacuation of residential areas and critical facilities as well as mechanisms such as streams and winds that can disperse contaminants beyond the primary incident scene. Similarly, flood damage curves provide information about the extent of damage expected in a given flood event, and HAZUS provides loss estimates for earthquakes.

For other manmade hazards such as bombs, however, damage analysis capabilities are still evolving and are not yet widely available within state and local governments. Software can be used to model blast effects on structures, but tools that can easily translate this information into loss estimates for mitigation purposes are not yet available. When dealing with these difficult-to-quantify risks, the planning team may wish to assume worst-case scenarios and estimate losses based on those scenarios using the techniques discussed in Step 3 of *Understanding Your Risks* (FEMA 386-2).

Using the results of your vulnerability analysis and your best estimates of potential losses, you can now formulate mitigation goals to drive the development of a mitigation strategy.

This worksheet is intended as an aid for identifying critical facilities, sites, systems, and other assets in your community or state. Check all the boxes that apply to your jurisdiction.

Local, state, and federal government offices
(list all in your jurisdiction)

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Military installations, including Reserve and National Guard component facilities (list all in your jurisdiction)

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Emergency services

- ☐ Backup facilities
- ☐ Communication centers
- ☐ Emergency operations centers
- ☐ Fire/Emergency Medical Service (EMS) facilities
- ☐ Law enforcement facilities

Politically or symbolically significant sites

- ☐ Embassies, consulates
- ☐ Landmarks, monuments
- ☐ Political party and special interest group offices
- ☐ Religious sites

Transportation infrastructure components

- ☐ Airports
- ☐ Bus stations
- ☐ Ferry terminals
- ☐ Interstate highways
- ☐ Oil/gas pipelines
- ☐ Railheads/rail yards
- ☐ Seaports/river ports
- ☐ Subways
- ☐ Truck terminals
- ☐ Tunnels/bridges

Energy, water, and related utility systems

- ☐ Electricity production, transmission, and distribution system components
- ☐ Oil and gas storage/shipment facilities
- ☐ Power plant fuel distribution, delivery, and storage
- ☐ Telecommunications facilities
- ☐ Wastewater treatment plants
- ☐ Water supply/purification/distribution systems

Telecommunications and information systems

- ☐ Cable TV facilities
- ☐ Cellular network facilities
- ☐ Critical cable routes
- ☐ Major rights of way
- ☐ Newspaper offices and production/distribution facilities
- ☐ Radio stations
- ☐ Satellite base stations
- ☐ Telephone trunking and switching stations
- ☐ Television broadcast stations

Health care system components

- ☐ Emergency medical centers
- ☐ Family planning clinics
- ☐ Health department offices
- ☐ Hospitals
- ☐ Radiological material and medical waste transportation, storage, and disposal
- ☐ Research facilities, laboratories
- ☐ Walk-in clinics

Financial services infrastructures and institutions

- ☐ Armored car services
- ☐ Banks and credit unions

Agricultural facilities

- ☐ Chemical distribution, storage, and application sites
- ☐ Crop spraying services
- ☐ Farms and ranches
- ☐ Food processing, storage, and distribution facilities

Commercial/manufacturing/industrial facilities

- ☐ Apartment buildings
- ☐ Business/corporate centers
- ☐ Chemical plants (include facilities having Section 302 Extremely Hazardous Substances on-site)
- ☐ Factories
- ☐ Fuel production, distribution, and storage facilities
- ☐ Hotels and convention centers
- ☐ Industrial plants
- ☐ Malls and shopping centers
- ☐ Raw material production, distribution, and storage facilities
- ☐ Research facilities, laboratories
- ☐ Shipping, warehousing, transfer, and logistical centers

Mobile assets

- ☐ Aviation and marine units
- ☐ Mobile emergency operations centers/command centers
- ☐ Portable telecommunications equipment
- ☐ Red Cross Emergency Response Vehicles, Salvation Army mobile canteens, etc.
- ☐ Other (Bloodmobiles, mobile health clinics, etc.)

Recreational facilities

- ☐ Auditoriums
- ☐ Casinos
- ☐ Concert halls and pavilions
- ☐ Parks
- ☐ Restaurants and clubs frequented by potential target populations
- ☐ Sports arenas and stadiums
- ☐ Theaters

Public/private institutions

- ☐ Academic institutions
- ☐ Cultural centers
- ☐ Libraries
- ☐ Museums
- ☐ Research facilities, laboratories

Events and attractions

- ☐ Festivals and celebrations
- ☐ Open-air markets
- ☐ Parades
- ☐ Rallies, demonstrations, and marches
- ☐ Religious services
- ☐ Scenic tours
- ☐ Theme parks

Facility Inherent Vulnerability Assessment Matrix

The Facility Inherent Vulnerability Assessment Matrix *provides a way to record how vulnerable each asset is and enables the planning team to compare how vulnerable the assets are relative to each other. Make a copy for each asset and fill in the facility name or other identifier in the space provided. Select the appropriate point value for each criterion based on the description in each row. Then add the point values to get the total for each asset. When you have done this for each asset you identified, compare the total scores to see how the assets rank in relation to one another.*

Facility _____

Vulnerability Point Values

Criteria	0	1	2	3	4	5	Score
Asset Visibility	–	Existence not well known	–	Existence locally known	–	Existence widely known	
Target Utility	None	Very Low	Low	Medium	High	Very High	
Asset Accessibility	Remote location, secure perimeter, armed guards, tightly controlled access	Fenced, guarded, controlled access	Controlled access, protected entry	Controlled access, unprotected entry	Open access, restricted parking	Open access, unrestricted parking	
Asset Mobility	–	Moves or is relocated frequently	–	Moves or is relocated occasionally	–	Permanent / fixed in place	
Presence of Hazardous Materials	No hazardous materials present	Limited quantities, materials in secure location	Moderate quantities, strict control features	Large quantities, some control features	Large quantities, minimal control features	Large quantities, accessible to non-staff persons	
Collateral Damage Potential	No risk	Low risk / limited to immediate area	Moderate risk / limited to immediate area	Moderate risk within 1-mile radius	High risk within 1-mile radius	High risk beyond 1-mile radius	
Site Population/ Capacity	0	1-250	251-500	501-1000	1001-5000	> 5000	
						TOTAL	

Increments may be adjusted to better reflect your response capabilities or to be consistent with other guidance such as Mass Casualty Incident plans. Note that different risks may exist at a facility depending on whether it is occupied or vacant.

Adapted from: FEMA Emergency Management Institute, *Terrorism Planning Course*

phase 3


organize resources
assess risks
develop a mitigation plan
implement the plan and monitor progress

3 develop a mitigation plan

Overview

The hazard identification and risk assessment described in Phase 2 will determine what facilities and systems in your jurisdiction are at highest risk. In Step 1 of Phase 3, you will develop goals and objectives for the protection of these assets to prevent or avoid an attack and to reduce losses in the event an attack occurs. Step 2 discusses the issues unique to identifying and prioritizing mitigation actions for terrorism and technological hazards. These actions primarily focus on creating a resilient, protective built environment. Step 3 highlights special considerations in developing an implementation strategy. Step 4 summarizes the important components to include in your terrorism and technological hazard mitigation plan. Cross-references are made to *Developing the Mitigation Plan: Identifying Mitigation Actions and Implementation Strategies* (FEMA 386-3).

Goals are general guidelines that identify what you want to achieve. They are usually long-term in nature.

Objectives define measurable strategies or implementation steps to attain a goal. They are shorter in range and more specific than goals.

Goals and objectives help determine where efforts and resources should be focused to maximize the effectiveness of mitigation-related activities. Whenever possible, mitigation goals and objectives should be multi-hazard in nature in order to provide the most comprehensive protection to your community or state. In addition to brainstorming, the planning team can identify additional goals and objectives in the following ways:

- **Review existing plans.** Review existing mitigation, comprehensive, and emergency plans, building upon and/or modifying existing initiatives to maximize coordination between plans and minimize conflicts and duplication of effort. To the extent possible, existing plans should be used to address the special problems posed by technological and other manmade hazards rather than generating new, stand-alone documents.
- **Solicit public opinions.** Including the community in identifying goals and objectives will help ensure buy-in when mitigation actions are selected, and both the media and the Internet can be valuable communication tools. There are a number of methods for gauging public opinion:
  - Establish working groups or advisory committees
  - Hold town hall meetings
  - Administer surveys
  - Hold facilitated meetings with community representatives

While all of these methods can be effective on their own, it may be advantageous to combine multiple strategies, such as surveys and town hall meetings, in order to obtain the advantages of both a structured questionnaire as well as a free-flowing discussion.

Step 1
Develop Mitigation Goals and Objectives

The process for developing the mitigation goals and objectives that will shape your implementation strategy is the same whether you are addressing natural or manmade hazards. As discussed in *Developing the Mitigation Plan: Identifying Mitigation Actions and Implementation Strategies* (FEMA 386-3), you will review the risk assessment and loss estimation findings to identify assets at greatest risk. Manmade risk information should be combined with the findings for natural hazards to create a comprehensive picture of your community or state's vulnerabilities to both natural and manmade hazards. Your terrorism and technological disaster mitigation goals, as with those for natural disasters, should strive to protect lives and property, reduce the costs of disaster response, and minimize disruption to the community or state following a disaster. See *Developing the Mitigation Plan* for more details on formulating and prioritizing your goals.

Sample Mitigation Goals and Objectives for Terrorism and Technological Hazard Mitigation

Goal 1: Reduce the community's risk of exposure to hazardous materials.

Objective 1: Install security measures at the anhydrous ammonia transfer and storage facility.

Objective 2: Increase the level of security of the facility using landscape design, lighting, and vehicle barriers.

Objective 3: Assess feasibility of hardening product storage and handling infrastructures.

Goal 2: Protect the community's water supply.

Objective 1: Install security measures at the city water treatment plant.

Objective 2: Secure all remote pump facilities.

Objective 3: Monitor for radiological, biological, and chemical contaminants.

Goal 3: Ensure that the city government has reliable communications systems.

Objective 1: Update the telecommunications capabilities of city government offices.

Objective 2: Create redundant/backup capability for landline telephone system.

Objective 3: Develop off-site backup of information technology systems.

Goal 4: Reduce risk to critical government facilities.

Objective 1: Increase vehicle standoff distance from the Emergency Operations Center.

Objective 2: Restrict parking and vehicle access to the underground parking garage at City Hall.

Step 2
Identify and Prioritize Mitigation Actions

Once you have developed goals and objectives for mitigation, you should identify specific actions to help you achieve them. As you consider mitigation options, keep in mind that attacks and accidents are functions of human activity, and the risk of such events is a characteristic of the target itself rather than of its geographic location. Clearly, there are areas in most communities where the chances of an attack or accident are considerably different from other parts of the jurisdiction—higher at industrial parks and critical facilities than in suburban residential neighborhoods, for example—but there is no such thing as a definable "terrorism zone" or "accident district" in the same sense as there are identifiable floodplains and seismic fault lines. Thus, it is not effective to protect people, buildings, and systems from manmade hazards by simply relocating them as one could for some natural disasters.

Rather than removing potential victims from the hazard, then, mitigation strategies for manmade hazards focus primarily on creating a built environment that is difficult to attack, resilient to the consequences of an attack or accident, and protective of its occupants should an incident occur. This can be accomplished through target hardening and other actions. Additional actions such as public awareness and education initiatives are not discussed in this guide but should be considered when formulating your mitigation strategy.

Target hardening actions range from small-scale projects, such as installing security fencing around an HVAC system's air intake, to community-wide initiatives, such as altering land use patterns to require buffer zones around campuses of high-risk buildings. Also, while some actions are highly specific in nature and function, others can meet multiple goals. For example, designing a building to resist the force of a bomb blast will also offer protection from windstorms, and requiring buffer zones around critical facilities can help meet open space requirements and protect wetlands. The planning team is encouraged to take advantage of these complementary approaches whenever possible.

Target hardening actions draw from a wide variety of disciplines, all of which, as discussed in Phase 1, should be represented on (or at least accessible to) the mitigation planning team. Potential hardening techniques and strategies are numerous, and a listing

Taking Advantage of Existing Processes, Strategies, and Tools

Some actions and techniques used for mitigating natural hazards may also provide protection against manmade hazards, such as:

Earthquake mitigation techniques that provide structural strengthening of buildings may help resist impact/explosion effects of bombs. Examples of such techniques include adding steel moment frames, shear walls, cross bracing, stronger floor systems, walls reinforced with shotcrete/fiber materials, columns reinforced with fiber wraps/steel jackets, tension/shear anchors, vibration dampers, and strengthening or providing additional detailing of the building's connections.

Fire mitigation techniques may help protect facilities against the effects of bombs and incendiary attacks. Examples of such techniques include improved sprinkler systems, increased use of fireproofing and/or fire-resistant materials, redundant water supplies for fire protection (day-to-day and alternative), and site setbacks.

High wind mitigation techniques that provide building envelope protection and structural strengthening may also help mitigate against impact/explosion effects of bombs. Examples of such techniques include openings using windows with impact-resistant laminated glazing, improving connections and the load path of the building, and adding/reinforcing shear walls.

Terrorism mitigation is becoming an integral part of multi-hazard mitigation, in process and often in practice. Additionally, an action that addresses the fullest possible spectrum of natural and manmade hazards will likely show the most cost-effectiveness.

The planning team should draw on all available sources of expertise when selecting specific actions, keeping in mind the overall objectives of maximizing opportunities for multi-hazard mitigation; promoting sustainability through choosing socially, economically, and environmentally beneficial solutions; supporting preparedness, response, and recovery; and ensuring cost-effectiveness.

of every possible action lies beyond the scope of this guidance. The list of potential actions provided below gives an overview of the techniques and strategies available. The Library in Appendix C contains references to many sources of information on these topics. The following section will discuss special considerations when evaluating actions to meet your goals and objectives.

Terrorism and Technological Hazard Mitigation Actions

The list of actions below is by no means exhaustive or definitive; rather, it is intended as a point of departure for identifying potential mitigation techniques and strategies in your community or state.

Site Planning and Landscape Design

- Implement Crime Prevention Through Environmental Design (CPTED)
- Minimize concealment opportunities in landscaping and street furniture, such as hedges, bus shelters, benches, and trash receptacles
- Design grounds and parking facilities for natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities
- Separate vehicle and pedestrian traffic
- Implement vehicle and pedestrian access control and inspection at perimeter (ensure ability to regulate flow of people and vehicles one at a time)
- Design site circulation to minimize vehicle speeds and eliminate direct approaches to structures
- Incorporate vehicle barriers such as walls, fences, trenches, ponds/basins, plantings, trees, sculptures, and fountains into site planning and design
- Ensure adequate site lighting
- Design signage for simplicity and clarity
- Locate critical offices away from uncontrolled public areas
- Separate delivery processing facilities from remaining buildings
- Maintain access for emergency responders, including large fire apparatus
- Identify and provide alternate water supplies for fire suppression
- Eliminate potential site access through utility tunnels, corridors, manholes, etc.

Architectural and Interior Space Planning

- Collocate/combine staff and visitor entrances; minimize queuing in unprotected areas
- Incorporate employee and visitor screening areas into planning and design
- Minimize device concealment opportunities such as mailboxes and trash receptacles outside screened areas
- Prohibit retail activities in non-secured areas
- Do not locate toilets and service spaces in non-secured areas
- Locate critical assets (people, activities, systems) away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Separate high-risk and low-risk activities
- Separate high-risk activities from areas accessible to the public
- Separate visitor activities from daily activities
- Separate building utilities from service docks, and harden utilities
- Locate delivery and mail processing facilities remotely or at exterior of building; prevent vehicles from driving into or under building
- Establish areas of refuge; ensure that egress pathways are hardened and discharge into safe areas
- Locate emergency stairwells and systems away from high-risk areas
- Restrict roof access
- Ensure that walls, doors, windows, ceilings, and floors can resist forced entry
- Provide fire- and blast-resistant separation for sprinkler/standpipe interior controls (risers) and key fire alarm system components
- Use visually open (impact-resistant, laminated glass) stair towers and elevators in parking facilities
- Design finishes and signage for visual simplicity

Structural Engineering

- Create blast-resistant exterior envelope
- Ensure that structural elements can resist blast loads and progressive collapse
- Install blast-resistant exterior window systems (frames, security films, and blast curtains)
- Ensure that other openings (vents, etc.) are secure and blast-resistant
- Ensure that mailrooms are secure and blast-resistant
- Enclose critical building components within hardened walls, floors, and ceilings

(continued)

Mechanical Engineering

- Locate utility and ventilation systems away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Protect utility lifelines (water, power, communications, etc.) by concealing, burying, or encasing
- Locate air intakes on roof or as high as possible; if not elevated, secure within CPTED-compliant fencing or enclosure
- Use motorized dampers to close air intakes when not operational
- Locate roof-mounted equipment away from building perimeter
- Ensure that stairways maintain positive pressure
- Provide redundant utility and ventilation systems
- Provide filtration of intake air
- Provide secure alternate drinking water supply

Electrical Engineering

- Locate utility systems and lifelines away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Implement separate emergency and normal power systems; ensure that backup power systems are periodically tested under load
- Locate primary and backup fuel supplies away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Secure primary and backup fuel supply areas
- Install exterior connection for emergency power
- Install adequate site lighting
- Maintain stairway and exit sign lighting
- Provide redundant telephone service
- Ensure that critical systems are not collocated in conduits, panels, or risers
- Use closed-circuit television (CCTV) security system

Fire Protection Engineering

- Ensure compliance with codes and standards, including installation of up-to-date fire alarm and suppression systems
- Locate fire protection water supply system critical components away from entrances, vehicle circulation and parking, and loading and maintenance areas
- Identify/establish secondary fire protection water supply
- Install redundant fire water pumps (e.g., one electric, one diesel); locate apart from each other
- Ensure adequate, redundant sprinkler and standpipe connections
- Install fire hydrant and water supply connections near sprinkler/standpipe connections
- Supervise or secure standpipes, water supply control valves, and other system components
- Implement fire detection and communication systems
- Implement redundant off-premises fire alarm reporting
- Locate critical documents and control systems in a secure yet accessible place
- Provide keybox near critical entrances for secure fire access
- Provide fire- and blast-resistant fire command center
- Locate hazardous materials storage, use, and handling away from other activities
- Implement smoke control systems
- Install fire dampers at fire barriers
- Maintain access to fire hydrants
- Maintain fire wall and fire door integrity
- Develop and maintain comprehensive pre-incident and recovery plans
- Implement guard and employee training
- Conduct regular evacuation and security drills
- Regularly evaluate fire protection equipment readiness/adequacy

Security

- Develop backup control center capabilities
- Secure electrical utility closets, mechanical rooms, and telephone closets
- Do not collocate security system wiring with electrical and other service systems
- Implement elevator recall capability and elevator emergency message capability
- Implement intrusion detection systems; provide 24-hour off-site monitoring
- Implement and monitor interior boundary penetration sensors
- Implement color closed-circuit television (CCTV) security system with recording capability
- Install call boxes and duress alarms
- Install public and employee screening systems (metal detectors, x-ray machines, or search stations)

Parking

- Minimize off-site parking on adjacent streets/lots and along perimeter
- Control all on-site parking with ID checks, security personnel, and access systems
- Separate employee and visitor parking
- Eliminate internal building parking
- Ensure natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities
- Use transparent/non-opaque walls whenever possible
- Prevent pedestrian access to parking areas other than via established entrances

While many benefits can be achieved through implementing mitigation actions, planners should be sensitive to potential negative impacts as well. For example, altering traffic patterns may increase commute times and distances, and reducing on-street parking may impact retail activity. Such considerations can be pivotal in determining the feasibility, viability, and potential for success of mitigation planning initiatives.

Prioritize Mitigation Actions

When prioritizing natural hazard mitigation actions, a benefit-cost analysis is generally conducted for each proposed action. Several factors are considered, including:

- Cost(s) of the mitigation action;
- Dollar value of risk reduction (i.e., loss of life, structure, content, and function) each time the hazard occurs (discussed in detail in *Understanding Your Risks: Identifying Hazards and Estimating Losses* [FEMA 386-2]);
- Frequency with which the benefits of the action will be realized (i.e., frequency of hazard occurrence); and
- Time value of money (i.e., the fact that benefits and costs in the future are worth less than benefits and costs today).

These factors are then combined by calculating the net present value of aggregate future benefits and costs over the life span of the action. For more details, see *Using Benefit-Cost Analysis in Mitigation Planning* (FEMA 386-5).

Three challenges arise when applying this benefit-cost framework to terrorism and technological disaster mitigation actions: (1) the probability of an attack or frequency of the hazard occurrence is not known; (2) the deterrence rate may not be known; and (3) the lifespan of the action may be difficult to quantify.

First, the frequency factor is much more complex in the case of manmade hazards than for natural hazards. While it is possible to estimate how often many natural disasters will occur (for example, a structure located in the 100-year floodplain is considered to have a 1 percent chance of being flooded in any given year), it is very difficult to quantify the likelihood of a terrorist attack or technological disaster. Quantitative methods to estimate these probabilities are being developed but have not yet been refined to the point where they can be used to determine incident probability on a facility-by-facility basis. Therefore, the planning team must use a qualitative approach based on threat and vulnerability considerations to estimate the relative likelihood of an attack or accident rather than the precise frequency. Such an approach is necessarily subjective but can be combined with quantitative estimates of cost-effectiveness (the cost of an action compared to the value of the lives and property it saves in a worst-case scenario) to help illustrate the overall risk reduction achieved by a particular mitigation action.

It is possible to determine fairly accurately how effective mitigation efforts will be in preventing damages from a given type of attack. The performance of many security and mitigation actions can be modeled using established engineering techniques. For example, structural engineers can determine how a hardening action will protect a building's envelope. Naturally, the effectiveness of actions that rely on personnel or complex hardware can be more difficult to ascertain. For example, what is the probability that a security guard will fall asleep or that lightning will disable a perimeter sensor system?

Second, the deterrence or preventative value of an action cannot be calculated if the number of incidents it averts is not known. Deterrence in the case of terrorism may also have a secondary impact in that once a potential target is hardened, a terrorist may turn to a less protected facility—changing the likelihood of an attack for both targets.

Third, the lifespan of a mitigation action presents another problem when carrying out a benefit-cost analysis for terrorism and technological hazards. Future benefits are generally calculated for a natural hazard mitigation action in part by estimating the number of times the action will perform successfully over the course of its useful life. However, some protective actions may be damaged or destroyed in a single manmade attack or accident. For example, blast-resistant window film may have performed to 100% effectiveness by preventing injuries from flying glass, but it may still need replacement after one "use." Other actions, such as a building setback, cannot be "destroyed" or "used up" per se. This is in contrast to many natural hazard mitigation actions, where the effectiveness and life span of a structural retrofit or land use policy are easily understood and their value over time quantifiable.

Step 3
Prepare an Implementation Strategy

As stated in the Foreword, this how-to guide assumes that your community or state is engaged in a natural hazards mitigation planning process and is intended to serve as a supplemental resource to help you address the unique risks associated with terrorism and technological hazards. If you have incorporated terrorism and technological hazards into a well-managed process, the implementation strategies and tools you use should enable you to effectively reduce your community or state's vulnerability to manmade disasters as well. *Developing the Mitigation Plan* (FEMA 386-3) provides more details on preparing an implementation strategy.

Step 4
Document the Mitigation Planning Process

The mitigation plan for manmade hazards will be based on the risk assessment conducted in Phase 2 and will include a comprehensive strategy to address the mitigation priorities developed in Phase 3, Step 2. This information, which should be integrated into the natural hazard mitigation plan, should include:

- A summary of the planning process, including the sequence of actions taken and a list of the team members and stakeholders who participated;
- The results of the risk assessment and loss estimation;
- Mitigation goals and objectives aimed at reducing or avoiding the effects of manmade hazards;
- Mitigation actions that will help the community or state accomplish the established goals and objectives; and
- Implementation strategies that detail how the mitigation actions will be implemented and administered.

The hazard mitigation plan should serve as the focal point and basis for mitigation decisions for *all* hazards—natural and manmade. As such, it should be written so that anyone who reads it can gain an understanding of current and future hazards and risks as well as the community's or state's intended solutions to those problems.

Ideally, terrorism and technological hazards will be incorporated into your existing mitigation plan; a single comprehensive plan is generally easier to manage and implement than a collection of stand-alone documents. However, some information may be of such high sensitivity that it should not be included in publicly available mitigation planning documents. Examples of such information include vulnerability studies of critical infrastructure and data on security plans and systems. This material should be treated as an addendum to the mitigation plan so that it is still part of the plan, but access to it can be controlled. For guidance on protecting sensitive information, see Phase 4, Consideration 1, Community Interest and Information Sensitivity.

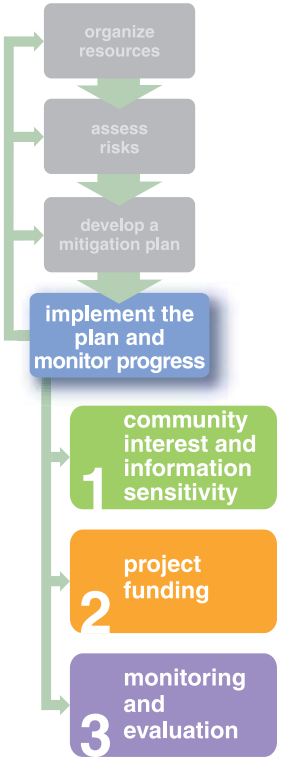

organize resources
assess risks
develop a mitigation plan
implement the plan and monitor progress

phase 4

4 implement the plan and monitor progress

Overview

The fourth phase of the mitigation planning process, *Implement the Plan and Monitor Progress*, describes how to bring the mitigation plan to life. The implementation and monitoring phase is largely the same across the entire spectrum of hazards and is discussed in detail in *Bringing the Plan to Life: Implementing the Hazard Mitigation Plan* (FEMA 386-4). This section will address special considerations for implementing mitigation actions unique to manmade hazards and should serve as a supplement to the process described in *Bringing the Plan to Life*.



Consideration 1 Community Interest and Information Sensitivity

As a result of the heightened level of interest in the vulnerability of American communities to terrorism following the events of September 11, 2001, the public is likely to be keenly interested in efforts to protect people, buildings, and systems from terrorism and technological disasters. The planning team should understand that this presents both benefits and challenges, because much of the same information that can be used to rally public support for mitigation planning can also be of use to potential terrorists, saboteurs, or others with malevolent intent. For that reason, the planning team must carefully maintain the security of any information that pertains to vulnerabilities, security measures, and response plans. Jurisdictions' legal counsels should be able to provide guidance on how best to protect such sensitive information within the provisions of applicable freedom of information laws.

This constitutes a significant departure from the open and inclusive way in which mitigation planning has historically been conducted. However, new security realities demand that we re-evaluate the way we think about information sensitivity, in particular how, where, when, and with whom we discuss risks, vulnerabilities, and protective (mitigation) actions. In addition to the overarching

public safety rationale for protecting this information from those who would use it against us, the planning team should be sensitive to the fact that the owners and operators of many community assets may be reluctant to reveal their own security shortcomings due to concerns about liability, perception of vulnerability or weakness, and general security-consciousness. For communities and states to work effectively with the people, facilities, and systems they are tasked with protecting, working relationships must be based on trust. All project partners should be committed to maintaining the integrity of the planning process as well as the principles and ultimate goal of the process: a more secure built environment.

Thus, managing sensitive information will be a new challenge for many communities and states. The federal government has the option to classify information when appropriate to protect the interest of national security, but most state and local governments currently lack adequate authorities and tools for preventing the inappropriate disclosure of every kind of sensitive data with any certainty. Communities and states should address this problem in two ways: first, they will need to ensure that sensitive information is handled in such a way as to maintain its security, and second, they will need to have adequate protections in place to ensure that sensitive information is not released when it is requested by members of the public who have no justifiable reason (or "need to know") for seeing the information. The following sections elaborate on these two ways to protect sensitive information while maintaining an appropriate level of public involvement in the planning process.

- **Internal handling procedures.** State and local governments may have the ability to assign "For Official Use Only" (FOUO) status or a similar designation to information that is privileged, sensitive, or otherwise should be protected from circulation or disclosure to the public. However, such actions often lack formal information handling procedures and enforceability. Communities are encouraged to review their handling procedures to ensure that sensitive information in their possession can be authoritatively designated as such and protected appropriately, and once proper procedures are in place they should be applied and adhered to rigorously.
- **Withholding sensitive information.** In keeping with the democratic tradition, federal and state laws generally

require that government proceedings and documents be accessible to the public. These laws, often called "sunshine laws" or "freedom of information" laws, usually require public access to meetings whenever a commission, committee, board, task force or other official group meets to discuss public business. They also require that most government documents and records be made available to the public upon request.

While these laws seek to keep governmental processes in the open, many of them establish disclosure exemptions for various types of sensitive information. Planners should work with their jurisdiction's legal staff to carefully review the applicable laws and to determine how these laws may impact their ability to protect sensitive planning information. Furthermore, they should also understand the specific procedures required to withhold documents and hold closed meetings as necessary to protect sensitive information from disclosure to anyone without a "need to know."

Suggested Elements and Sample Language for a "For Official Use Only" (FOUO) Policy

- **Definition of FOUO**

  The term 'For Official Use Only' should apply to information which is sensitive and requires protection from disclosure to the general public, and for which a significant reason, statutory requirement, or regulatory instruction exists to preclude general circulation. FOUO status is not a security classification level.

- **Guidelines for determining sensitivity**

  Information that may qualify for FOUO status includes the design, construction, security, and protection of government facilities and critical infrastructures; assessments of the vulnerabilities of facilities and systems; plans, procedures, and protocols for responding to terrorist attacks or other criminal events; or any other information that could be used for the purposes of damaging or destroying any facility or disrupting any operations.

- **Designation of authority**

  Authority to assign and remove FOUO status should be granted to designated personnel based on position and/or responsibilities.

- **Document marking requirements**

  Information that has been designated FOUO should be plainly marked as such for ease of recognition. To promote proper protection of information, markings should be applied at the time documents are drafted or as soon as FOUO information is added. Materials containing FOUO information should be marked

  'PROPERTY OF (JURISDICTION NAME)
  FOR OFFICIAL USE ONLY'

  at the bottom of the front cover, title page, first page and outside of the back cover. Additionally, each page containing FOUO information should be similarly marked at the bottom. Material other than paper documents such as slides, computer media, films, etc., should also bear these markings. Electronically transmitted messages (e.g., e-mails) containing FOUO information should have the abbreviation 'FOUO' before the beginning of the text.

- **Handling instructions**

  FOUO material should never be left unattended, and reasonable steps should be taken to minimize the risk of access by anyone without a "need to know." After working hours, FOUO information should be stored in a locked desk, file cabinet, bookcase, or similar location. Restrictions may also be placed on the duplication and transmission of FOUO information.

Federal Funding for Manmade Hazard Mitigation Projects

At the time of this writing, there is little federal funding specifically earmarked for state and local use in mitigating against manmade hazards. When dealing with multiple sources of funding, ensure that you seek funding from the most directly appropriate and relevant program before seeking assistance from other sources. That said, mitigation against terrorism and technological hazards will require creative funding strategies that incorporate a variety of non-traditional sources. Three reasons for this are:

1. Terrorism can potentially occur almost anywhere and can affect a wide range of facilities and systems;
2. As with natural hazard mitigation, the development and implementation of antiterrorism strategies can be complex and expensive; and
3. Comprehensive antiterrorism and technological hazard mitigation includes security measures and other techniques that may not be eligible for FEMA funding under current regulations.

Security considerations should be a priority in all capital improvement projects including both renovation and new development.

Consideration 2 Project Funding

Increasingly, communities are challenged by budget constraints that require "doing more with less." While many pre- and post-disaster funding sources exist that can help communities strengthen themselves against natural disasters, creativity will be the key to identifying how mitigation plans and actions for terrorism and technological hazards can be funded.

- **Local governments** have a good opportunity for incorporating mitigation funding into long-range planning, especially in the capital improvement budget process. For example, planning for a new municipal building is an ideal opportunity to site a critical facility in a low hazard area, to ensure that it is built with seismic, high wind, or other appropriate hazard resistance as applicable, and to incorporate security systems and security-oriented design principles into the facility's planning and design.
- **State governments** can implement incentive programs using tax rebates and budget surpluses to promote mitigation actions and strengthen building codes. They can also incorporate all-hazard mitigation considerations into the processes, guidance, and requirements that they develop for comprehensive planning, capital improvement planning, urban design, land development regulation, growth management, and sustainability.
- **Federal government** funding for terrorism-related activities is rapidly expanding following the events of September 11, 2001. Many funding streams that may be of use to states and communities working to reduce their vulnerability to manmade hazards are not yet in place, but other established funding mechanisms not previously used for this purpose can be leveraged to provide assistance. Detailed information on available federal funding can be found in the Catalog of Federal Domestic Assistance at www.cfda.gov.
- **Private sector organizations**, businesses, and individual homeowners have much to gain from reducing their own risk by implementing cost-effective actions to increase security and survivability. Industrial partners and other private interests may be willing to contribute time, labor, materials, or other support if they are

convinced that the mitigation effort will benefit their organization as part of an overall community improvement.

Consideration 3
Monitoring and Evaluation

There are significant challenges to monitoring and evaluating the implementation of mitigation strategies for terrorism and technological hazards. Given the relatively low likelihood of manmade disasters occurring in most communities (particularly in contrast to many naturally occurring events), the value and effectiveness of mitigation actions such as structural blast-resistance retrofits and land use regulations may never be realized. Other actions such as the application of Crime Prevention Through Environmental Design techniques may indeed function to their full level of performance but their deterrent or preventative value may go unrecognized if they averted an incident that was, as a result, undetected. Still others such as guards and intrusion sensors may be put to the test regularly, either as part of a routine testing, training, and maintenance program or in "real world" events. Should an incident or accident occur, however, there will likely be significant interest on the part of the government, engineering, design, and standards communities in the performance of various actions, and the resulting inquiries and studies can provide valuable input into subsequent mitigation planning initiatives.

The monitoring and evaluation of the manmade hazards portion of the mitigation plan should correspond with the schedule established for the natural hazards portion of the plan. The plan should be revisited, and if necessary updated, on a regular basis to ensure that it is still relevant and accurate. If a disaster occurs, the plan should be revisited, and perhaps revised, then as well.

afterword

afterword

The basics of mitigating hazards before they become disasters are similar for both natural and manmade hazards. Whether you are confronting wind, water, seismicity, terrorism, hazardous materials, or sabotage, you can use the same four-phase mitigation planning process to reduce the consequences should these hazards impact the built environment. While communities of all sizes are increasingly aware of their vulnerability to manmade hazards, this awareness is of no value unless it is translated into action.

You may not be able to prevent every accident or deliberate attack, but a well planned and effectively implemented mitigation program will help to reduce the consequences of such incidents. Of course, the reality is that natural hazards may indeed present a much greater risk than terrorism and technological disasters due to their higher frequency of occurrence. By using this guide and the other how-to guides in the series, you will be able to identify, prioritize, and implement mitigation actions across the full spectrum of hazards and maximize the efficient allocation of public resources.

appendices

appendix a
acronyms

BCA	Benefit-Cost Analysis
CAMEO	Computer-Aided Management of Emergency Operations
CCTV	Closed-Circuit Television
CERT	Community Emergency Response Team
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CPTED	Crime Prevention Through Environmental Design
DMA	Disaster Mitigation Act of 2000
DOS	Department of State
EOP	Emergency Operating Plan
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GSA	General Services Administration
HAZUS	Hazards US
HIRA	Hazard Identification and Risk Assessment
HVAC	Heating, Ventilation, and Air Conditioning
IEMS	Integrated Emergency Management System
LEPC	Local Emergency Planning Committee
NBC	Nuclear, Biological, and Chemical
PCCIP	President's Commission on Critical Infrastructure Protection
SCADA	Supervisory, Control, and Data Acquisition
WMD	Weapons of Mass Destruction

appendix b
glossary

Antiterrorism Defensive measures used to reduce the vulnerability of individuals, forces, and property to terrorist acts. (Source: US Department of Defense, *Report of the Secretary of Defense to the President and the Congress*, 2000.)

Counterterrorism Offensive measures taken to prevent, deter, and respond to terrorism. (Source: US Department of Defense, *Report of the Secretary of Defense to the President and the Congress*, 2000.)

Crime Prevention Through Environmental Design (CPTED) A crime prevention strategy based on evidence that the design and form of the built environment can influence human behavior. Specifically, CPTED seeks to create a physical environment that discourages criminal activity. CPTED's basic principles are territoriality, access control, surveillance, activity support, and property maintenance.

Critical Infrastructure System whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation. (Source: U.S. Critical Infrastructure Assurance Office at http://www.ciao.gov/resource/index.html.)

Domestic Terrorism The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives. (Source: FBI, *Terrorism in the United States* 1998.)

Goals General guidelines that identify what you want to achieve. They are usually long-term in nature.

International Terrorism Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. (Source: FBI, *Terrorism in the United States* 1998.)

Mitigate To cause to become less harsh or hostile; to make less severe or painful.

Objectives Measurable strategies or implementation steps to attain a goal. They are shorter in range and more specific than goals.

Planning The act or process of making or carrying out plans; the establishment of goals, policies, and procedures for a social or economic unit.

Situational Crime Prevention A crime prevention strategy based on reducing the opportunities for crime by increasing the effort required to commit a crime, increasing the risks associated with committing the crime, and reducing the target appeal or vulnerability (whether property or person). This opportunity reduction is achieved by management and use policies such as procedures and training, as well as physical approaches such as alteration of the built environment.

Terrorism The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (Source: 28 CFR Section 0.85.)

Weapons of Mass Destruction (WMD) Explosive, incendiary, nuclear, biological, and chemical weapons. As defined in 18 U.S.C., Section 2332a,

"the term 'weapon of mass destruction' means –

(A) any destructive device as defined in section 921 of this title;

(B) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;

(C) any weapon involving a disease organism; or

(D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life."

Furthermore, a 'destructive device' is defined in 18 U.S.C., Section 921 as:

"any explosive, incendiary, or poison gas –

(i) bomb,

(ii) grenade,

(iii) rocket having a propellant charge of more than four ounces,

(iv) missile having an explosive or incendiary charge of more than one-quarter ounce,

(v) mine, or

(vi) device similar to any of the devices described in the preceding clauses."

appendix c
library

Research and Publications

American Planning Association. 1995. Integrating Emergency Management and the Planning Process. *City Planning and Management News,* Winter 1994-95: 3-4.

American Society of Civil Engineers. 1999. *Structural Design for Physical Security: State of the Practice.* Reston, VA: American Society of Civil Engineers.

Archibald, Rae W., et al. 2002. *Security and Safety in Los Angeles High-Rise Buildings after 9/11.* Santa Monica, California: RAND. (Online) Available at http://www.rand.org/publications/DB/DB381.

Britton, Neil R. and John Lindsay. 1995. Demonstrating the Need to Integrate City Planning and Emergency Preparedness: Two Case Studies. *International Journal of Mass Emergencies and Disasters* 13,2: 161-178.

Clarke, Ronald V., ed. 1997. *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Guilderland, N.Y.: Harrow and Heston.

Coleman, Michael A. 1997. *The Influence of Traffic Calming Devices upon Fire Vehicle Travel Times*. Washington, D.C.: Institute of Transportation Engineers.

Crowe, Timothy D. 2000. *Crime Prevention Through Environmental Design: Applications Of Architectural Design And Space Management Concepts* (2nd ed.). Stoneham, MA: Butterworth-Heinemann.

Federal Emergency Management Agency. 2002. *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations* (FEMA 403). Washington, D.C.: Federal Emergency Management Agency.

Federal Emergency Management Agency. 2001. *Mitigation Resources for Success (CD-ROM)* (FEMA 372). Washington, D.C.: Federal Emergency Management Agency.

Federal Emergency Management Agency. 2000. *Planning for a Sustainable Future: The Link Between Hazard Mitigation and Livability* (FEMA 364). Washington, D.C.: Federal Emergency Management Agency. (Online) Available at http://www.fema.gov/fima/planning_toc.shtm.

Federal Emergency Management Agency. 1997. *Radiological Emergency Management Independent Study Course* (IS-301). Washington, D.C.: Federal Emergency Management Agency. (Online) Available at http://training.fema.gov/EMIWeb/IS/is301.htm.

Federal Emergency Management Agency. 1996. *The Oklahoma City Bombing: Improving Building Performance through Multi-Hazard Mitigation* (FEMA 277). Washington, D.C.: Federal Emergency Management Agency.

Fehr, Stephen C. 1996. Parking Under Siege in D.C.: U.S. Anti-Terrorism Plan Threatens 360 Spaces. *The Washington Post*, July 13, 1996.

Fleissner, Dan and Fred Heinzelmann. 1996. *Crime Prevention Through Environmental Design and Community Policing*. Washington, D. C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (Online) Available at http://www.ncjrs.org/pdffiles/crimepre.pdf.

Gordon, Corey L. and William Brill. 1996. *The Expanding Role of Crime Prevention Through Environmental Design in Premises Liability*. Washington, D. C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (Online) Available at http://www.ncjrs.org/pdffiles/cptedlia.pdf.

Hart, Sara. 2002. In the aftermath of September 11, the urban landscape appears vulnerable and random: Architects and consultants focus on risk assessment and security through design. *Architectural Record*, March 2002.

Hinman, Eve E. and David J. Hammond. 1997. *Lessons from the Oklahoma City Bombing: Defensive Design Techniques*. Reston, VA: American Society of Civil Engineers (ASCE Press).

Lasley, James. 1998. *"Designing Out" Gang Homicides and Street Assaults*. Washington, D. C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (Online) Available at http://www.ncjrs.org/pdffiles/173398.pdf.

La Vigne, Nancy G. 1997. *Visibility and Vigilance: Metro's Situational Approach to Preventing Subway Crime*. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (Online) Available at http://www.ncjrs.org/pdffiles/166372.pdf.

Mulder, Kathy. 1998. *Split Speed Bump*. Washington, D.C.: Institute of Transportation Engineers.

National Capital Planning Commission. 2002. *The National Capital Urban Design and Security Plan*. (Online) Available at http://www.ncpc.gov/publications/UDSP/final%20UDSP.pdf.

National Capital Planning Commission. 2001. *Designing for Security in the Nation's Capital*. (Online) Available at http://www.ncpc.gov/planning_init/security/designingsec.pdf.

National Institute for Occupational Safety and Health. 2002. *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks* (DHHS (NIOSH) Publication No. 2002-139). Cincinnati, Ohio: National Institute for Occupational Safety and Health. (Online) Available at http://www.cdc.gov/niosh/bldvent/2002-139.html.

National League of Cities. 2000. *Domestic Terrorism: Resources for Local Governments*. Washington, DC.: National League of Cities.

National Research Council. 2001. *Protecting Buildings and People from Terrorism: Technology Transfer for Blast-effects Mitigation*. Washington, D.C.: National Academy Press.

Newman, Oscar. 1996. *Creating Defensible Space*. Washington, D.C.: U.S. Department of Housing and Urban Development. (Online) Available at http://www.huduser.org/publications/pdf/def.pdf.

Schneider, Richard H., and Ted Kitchen. 2002. *Planning for Crime Prevention: A Transatlantic Perspective*. New York, New York: Routledge.

Schwab, Jim, et al. 1998. *Planning for Post-Disaster Recovery and Reconstruction* (Planning Advisory Service Report Number 483/484). Chicago, Illinois: American Planning Association.

Sidell, Frederick R., et al. 1998. *Jane's Chem-Bio Handbook*. Alexandria, Virginia: Jane's Information Group.

Smith, Keith. 1992. *Environmental Hazards: Assessing Risk and Reducing Disaster*. New York, New York: Routledge.

Smith, Mary S. 1996. *Crime Prevention Through Environmental Design in Parking Facilities*. Washington, D. C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (Online) Available at http://www.ncjrs.org/pdffiles/cptedpkg.pdf.

Steinberg, Michele and Burby, Raymond J. 2002. Growing Safe. *Planning* 68,4: 22-23.

Taylor, Ralph B. and Adele V. Harrell. 1996. *Physical Environment and Crime*. Washington, D. C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (Online) Available at http://www.ncjrs.org/pdffiles/physenv.pdf.

U.S. Air Force. *Installation Force Protection Guide*. (Online) Available at http://www.afcee.brooks.af.mil/dc/dcd/arch/force.pdf.

U.S. Army. 2001. *Field Manual 3-19.30, Physical Security*. Washington, D.C.: Headquarters, Department of the Army. (Online) Available at http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/fm3-19.30.pdf.

U.S. Department of Justice. 1995. *Vulnerability Assessment of Federal Facilities*. (Online) Available at http://www.oca.gsa.gov.

U.S. Department of the Treasury, Bureau of Alcohol, Tobacco and Firearms. 1999. *Vehicle Bomb Explosion Hazard And Evacuation Distance Table*s. This publication is no longer available online. To request a copy, write to Bureau of Alcohol, Tobacco, Firearms and Exposives, Arson and Explosives Programs Division, 800 K Street, NW, Tech World Suite 710, Washington, DC 20001.

U.S. Environmental Protection Agency. 2001. *LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan.* (Online) Available at http://www.epa.gov/swercepp/factsheets/lepcct.pdf.

U.S. General Accounting Office. 2002. *Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities* (GAO-02-472T). (Online) Available at http://www.gao.gov/new.items/d02472t.pdf.

U.S. General Accounting Office. 2001. *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts* (GAO-02-208T). (Online) Available at http://www.gao.gov/new.items/d02208t.pdf.

U.S. General Accounting Office. 2001. *Homeland Security: Key Elements of a Risk Management Approach* (GAO-02-150T). (Online) Available at http://www.gao.gov/new.items/d02150t.pdf.

U.S. General Accounting Office. 2000. *Combating Terrorism: Linking Threats to Strategies and Resources* (T-NSIAD-00-218). (Online) Available at http://www.gao.gov/archive/2000/ns00218t.pdf.

U.S. General Services Administration. 2002. *GSA Occupant Emergency Program (OEP) Guide.* (Online) Available at http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/GSA_OEP_Guide_6.doc.

U.S. House of Representatives. 1996. *Impacts of the closure of Pennsylvania Avenue on the District of Columbia.* Hearing before the Subcommittee on the District of Columbia of the Committee on Government Reform and Oversight, House of Representatives, One Hundred Fourth Congress, second session, June 7, 1996. Washington, D.C.: U.S. Government Printing Office.

Web Sites

American Institute of Architects: Building Security Through Design	http://www.aia.org/security
American Lifelines Alliance	http://www.americanlifelinesalliance.org
American Society for Industrial Security	http://www.asisonline.org
Building Owners and Managers Association: BOMA International Emergency Resource Center	http://www.boma.org/emergency
Catalog of Federal Domestic Assistance	http://www.cfda.gov
Catalog of Federal Domestic Assistance: terrorism-related funding	http://www.cfda.gov/911.htm
Critical Infrastructure Assurance Office	http://www.ciao.gov
Critical Infrastructure Assurance Office: Critical Infrastructure Protection	http://www.ciao.gov/resource/pccip/pccip_documents.htm
Federal Emergency Management Agency: Emergency Management Institute, Terrorism Training and Resources	http://training.fema.gov/EMIWeb/terrorisminfor/ctrt.asp
Federal Emergency Management Agency: Mitigation Planning	http://www.fema.gov/fima/planning.shtm
Federal Emergency Management Agency: Information on manmade hazards	http://www.fema.gov/hazards
General Services Administration: Facilities Standards for the Public Buildings Service (note: certain information is excluded from public access for security reasons, but a vast amount of helpful guidance is available)	http://hydra.gsa.gov/pbs/pc/facilitiesstandards
General Services Administration: Office of the Chief Architect	http://www.oca.gsa.gov
General Services Administration, Public Buildings Service: First Impressions – Streamlining Security	http://hydra.gsa.gov/pbs/firstimpressions/takingaction/streamline_security.html
International Facility Management Association	http://www.ifma.org
Lawrence Berkeley National Laboratory: Advice for Safeguarding Buildings Against Chemical or Biological Attack	http://securebuildings.lbl.gov
National Capital Planning Commission: Security and Urban Design	http://www.ncpc.gov/planning_init/security/security.html
National Infrastructure Protection Center	http://www.nipc.gov
National Institute of Building Sciences	http://www.nibs.org

Penn State University, Protective Technology Center: Modern Protective Structures course	http://www.cde.psu.edu/C&I/ProtectiveStructures/default.html
Public Entity Risk Institute	http://www.riskinstitute.org
The Infrastructure Security Partnership	http://www.tisp.org
U.S. Army Corps of Engineers Center of Expertise for Protective Design: Blast Mitigation Action Group	http://bmag.nwo.usace.army.mil
U.S. Army Soldiers' and Biological Chemical Command: Basic Information on Building Protection	http://buildingprotection.sbccom.army.mil/basic
U.S. Department of Defense: Force Protection Equipment Demonstration IV	http://www.fped4.org
U.S. Department of Defense and U.S. Department of State: Technical Support Working Group	http://www.tswg.gov
U.S. Department of Energy, Sandia National Laboratories: Architectural Surety Program	http://www.sandia.gov/archsur
U.S. Department of Energy, Sandia National Laboratories: Critical Infrastructure Protection initiative	http://www.sandia.gov/LabNews/LN02-11-00/steam_story.html
U.S. Department of Justice, Federal Bureau of Investigation: Terrorism in the United States reports	http://www.fbi.gov/publications/terror/terroris.htm
U.S. Environmental Protection Agency: Chemical Emergency Preparedness and Prevention Office	http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/index.html
U.S. Fire Administration	http://www.usfa.fema.gov
U.S. General Accounting Office: Special Collections – Terrorism	http://www.gao.gov/terrorism.html
U.S. Navy, Naval Facilities Engineering Service Center, Security Engineering Division: Systematic Approach for Reviewing Projects for Protection Against Terrorism 3-day workshop	http://atfp.nfesc.navy.mil/training.htm
Whole Building Design Guide: Provide Security to Assets	http://www.wbdg.org (click “Design Guidance” then “Design Objectives” then “Secure/Safe”)

appendix d
worksheets

Worksheet #1 Build the Planning Team

Worksheet #2 Asset Identification Checklist

Worksheet #3 Facility Inherent Vulnerability Assessment Matrix

Step 2 of Getting Started *(FEMA 386-1) discusses establishing a planning team with a broad range of backgrounds and experience represented. This worksheet suggests additional individuals, agencies, and organizations that should be included on a team to plan for manmade hazards. State organizations can be included on local teams when appropriate to serve as a source of information and to provide guidance and coordination.*

You should use the checklist as a starting point for expanding your team.

	ON TEAM	ADD TO TEAM
Specialists for Manmade Hazards		
Bomb and Arson Squads	☐	☐
Community Emergency Response Teams	☐	☐
Hazardous Materials Experts	☐	☐
Infrastructure Owners/Operators	☐	☐
National Guard Units	☐	☐
Representatives from facilities identified in Worksheet #2: Asset Identification Checklist	☐	☐
Local/Tribal		
Administrator/Manager's Office	☐	☐
Budget/Finance Office	☐	☐
Building Code Enforcement Office	☐	☐
City/County Attorney's Office	☐	☐
Economic Development Office	☐	☐
Emergency Preparedness Office	☐	☐
Fire and Rescue Department	☐	☐
Hospital Management	☐	☐
Local Emergency Planning Committee	☐	☐
Planning and Zoning Office	☐	☐
Police/Sheriff's Department	☐	☐
Public Works Department	☐	☐
Sanitation Department	☐	☐
School Board	☐	☐
Transportation Department	☐	☐
Tribal Leaders	☐	☐

	ON TEAM	ADD TO TEAM
Special Districts and Authorities		
Airport and Seaport Authorities	☐	☐
Business Improvement District(s)	☐	☐
Fire Control District	☐	☐
Flood Control District	☐	☐
Redevelopment Agencies	☐	☐
Regional/Metropolitan Planning Organization(s)	☐	☐
School Districts	☐	☐
Transit/Transportation Agencies	☐	☐
Others		
Architectural/Engineering/Planning Firms	☐	☐
Citizen Corps	☐	☐
Colleges/Universities	☐	☐
Land Developers	☐	☐
Major Employers/Businesses	☐	☐
Professional Associations	☐	☐
Retired Professionals	☐	☐
State		
Adjutant General's Office (National Guard)	☐	☐
Board of Education	☐	☐
Building Code Office	☐	☐
Climatologist	☐	☐
Earthquake Program Manager	☐	☐
Economic Development Office	☐	☐

	ON TEAM	ADD TO TEAM
Emergency Management Office/ State Hazard Mitigation Officer	☐	☐
Environmental Protection Office	☐	☐
Fire Marshal's Office	☐	☐
Geologist	☐	☐
Homeland Security Coordinator's Office	☐	☐
Housing Office	☐	☐
Hurricane Program Manager	☐	☐
Insurance Commissioner's Office	☐	☐
National Flood Insurance Program Coordinator	☐	☐
Natural Resources Office	☐	☐
Planning Agencies	☐	☐
Police	☐	☐
Public Health Office	☐	☐
Public Information Office	☐	☐
Tourism Department	☐	☐

Non-Governmental Organizations (NGOs)	ON TEAM	ADD TO TEAM
American Red Cross	☐	☐
Chamber of Commerce	☐	☐
Community/Faith-Based Organizations	☐	☐
Environmental Organizations	☐	☐
Homeowners Associations	☐	☐
Neighborhood Organizations	☐	☐
Private Development Agencies	☐	☐
Utility Companies	☐	☐
Other Appropriate NGOs	☐	☐

This worksheet is intended as an aid for identifying critical facilities, sites, systems, and other assets in your community or state. Check all the boxes that apply to your jurisdiction.

Local, state, and federal government offices
(list all in your jurisdiction)

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Military installations, including Reserve and National Guard component facilities (list all in your jurisdiction)

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Emergency services

- ☐ Backup facilities
- ☐ Communication centers
- ☐ Emergency operations centers
- ☐ Fire/Emergency Medical Service (EMS) facilities
- ☐ Law enforcement facilities

Politically or symbolically significant sites

- ☐ Embassies, consulates
- ☐ Landmarks, monuments
- ☐ Political party and special interest group offices
- ☐ Religious sites

Transportation infrastructure components

- ☐ Airports
- ☐ Bus stations
- ☐ Ferry terminals
- ☐ Interstate highways
- ☐ Oil/gas pipelines
- ☐ Railheads/rail yards
- ☐ Seaports/river ports
- ☐ Subways
- ☐ Truck terminals
- ☐ Tunnels/bridges

Energy, water, and related utility systems

- ☐ Electricity production, transmission, and distribution system components
- ☐ Oil and gas storage/shipment facilities
- ☐ Power plant fuel distribution, delivery, and storage
- ☐ Telecommunications facilities
- ☐ Wastewater treatment plants
- ☐ Water supply/purification/distribution systems

Telecommunications and information systems

- ☐ Cable TV facilities
- ☐ Cellular network facilities
- ☐ Critical cable routes
- ☐ Major rights of way
- ☐ Newspaper offices and production/distribution facilities
- ☐ Radio stations
- ☐ Satellite base stations
- ☐ Telephone trunking and switching stations
- ☐ Television broadcast stations

Health care system components

- ☐ Emergency medical centers
- ☐ Family planning clinics
- ☐ Health department offices
- ☐ Hospitals
- ☐ Radiological material and medical waste transportation, storage, and disposal
- ☐ Research facilities, laboratories
- ☐ Walk-in clinics

Financial services infrastructures and institutions

- ☐ Armored car services
- ☐ Banks and credit unions

Agricultural facilities

- ☐ Chemical distribution, storage, and application sites
- ☐ Crop spraying services
- ☐ Farms and ranches
- ☐ Food processing, storage, and distribution facilities

Commercial/manufacturing/industrial facilities

- ☐ Apartment buildings
- ☐ Business/corporate centers
- ☐ Chemical plants (include facilities having Section 302 Extremely Hazardous Substances on-site)
- ☐ Factories
- ☐ Fuel production, distribution, and storage facilities
- ☐ Hotels and convention centers
- ☐ Industrial plants
- ☐ Malls and shopping centers
- ☐ Raw material production, distribution, and storage facilities
- ☐ Research facilities, laboratories
- ☐ Shipping, warehousing, transfer, and logistical centers

Mobile assets

- ☐ Aviation and marine units
- ☐ Mobile emergency operations centers/command centers
- ☐ Portable telecommunications equipment
- ☐ Red Cross Emergency Response Vehicles, Salvation Army mobile canteens, etc.
- ☐ Other (Bloodmobiles, mobile health clinics, etc.)

Recreational facilities

- ☐ Auditoriums
- ☐ Casinos
- ☐ Concert halls and pavilions
- ☐ Parks
- ☐ Restaurants and clubs frequented by potential target populations
- ☐ Sports arenas and stadiums
- ☐ Theaters

Public/private institutions

- ☐ Academic institutions
- ☐ Cultural centers
- ☐ Libraries
- ☐ Museums
- ☐ Research facilities, laboratories

Events and attractions

- ☐ Festivals and celebrations
- ☐ Open-air markets
- ☐ Parades
- ☐ Rallies, demonstrations, and marches
- ☐ Religious services
- ☐ Scenic tours
- ☐ Theme parks

Worksheet #3
Facility Inherent Vulnerability Assessment Matrix

The Facility Inherent Vulnerability Assessment Matrix *provides a way to record how vulnerable each asset is and enables the planning team to compare how vulnerable the assets are relative to each other. Make a copy for each asset and fill in the facility name or other identifier in the space provided. Select the appropriate point value for each criterion based on the description in each row. Then add the point values to get the total for each asset. When you have done this for each asset you identified, compare the total scores to see how the assets rank in relation to one another.*

Facility _____

Vulnerability Point Values

Criteria	0	1	2	3	4	5	Score
Asset Visibility	–	Existence not well known	–	Existence locally known	–	Existence widely known	
Target Utility	None	Very Low	Low	Medium	High	Very High	
Asset Accessibility	Remote location, secure perimeter, armed guards, tightly controlled access	Fenced, guarded, controlled access	Controlled access, protected entry	Controlled access, unprotected entry	Open access, restricted parking	Open access, unrestricted parking	
Asset Mobility	–	Moves or is relocated frequently	–	Moves or is relocated occasionally	–	Permanent / fixed in place	
Presence of Hazardous Materials	No hazardous materials present	Limited quantities, materials in secure location	Moderate quantities, strict control features	Large quantities, some control features	Large quantities, minimal control features	Large quantities, accessible to non-staff persons	
Collateral Damage Potential	No risk	Low risk / limited to immediate area	Moderate risk / limited to immediate area	Moderate risk within 1-mile radius	High risk within 1-mile radius	High risk beyond 1-mile radius	
Site Population/ Capacity	0	1-250	251-500	501-1000	1001-5000	> 5000	
						TOTAL	

Increments may be adjusted to better reflect your response capabilities or to be consistent with other guidance such as Mass Casualty Incident plans. Note that different risks may exist at a facility depending on whether it is occupied or vacant.

Adapted from: FEMA Emergency Management Institute, *Terrorism Planning Course*

Those who cannot remember the past are condemned to repeat it

George Santayana

FEMA

September 2003
FEMA 386-7
Version 2.0