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 human-caused hazards fall into two general categories: terrorism (intentional acts) and technological hazards (accidental events). These two categories include the following hazards:

Terrorism

- Conventional bomb
- 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 human-caused 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 human-caused 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 human-caused 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 human-caused 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 Human-Caused Hazards

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

http://training.fema.gov/EMIWeb/ctrt.htm
(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 human-caused hazards can impact communities.

Step 2
Profile Hazard Events

In the area of hazard profiling, there are significant differences between natural and human-caused 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 human-caused 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 measures can be taken to reduce or eliminate the resulting damage.

Whether intentional or accidental, human-caused 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 human-caused 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 human-caused 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	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.	Energy decreases logarithmically as a function of distance from seat of blast. 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 human-caused 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 human-caused 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 human-caused 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 human-caused hazards and their potential consequences. Maps may not be able to actually predict where human-caused 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 eight critical infrastructure categories include:

1. Telecommunications infrastructure
2. Electrical power systems
3. Gas and oil facilities
4. Banking and finance institutions
5. Transportation networks
6. Water supply systems
7. Government services
8. Emergency services

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 eight 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 measures 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?

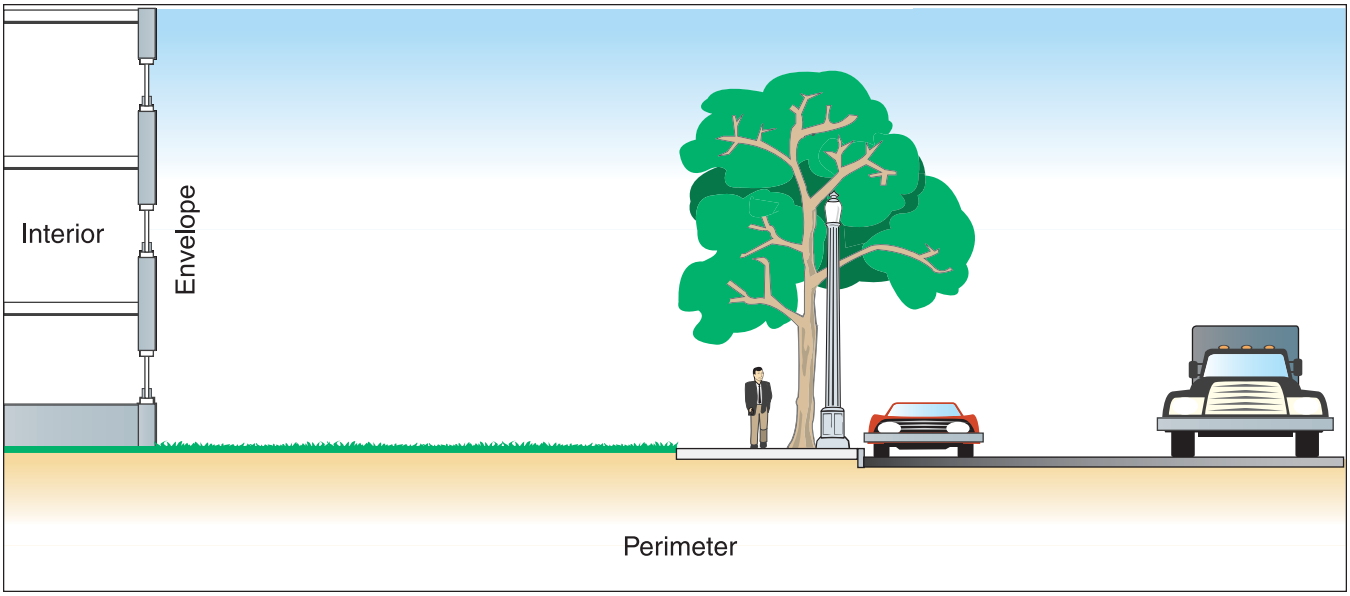
Building Envelope

- *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 measures 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 human-caused 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 eight 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 measure 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

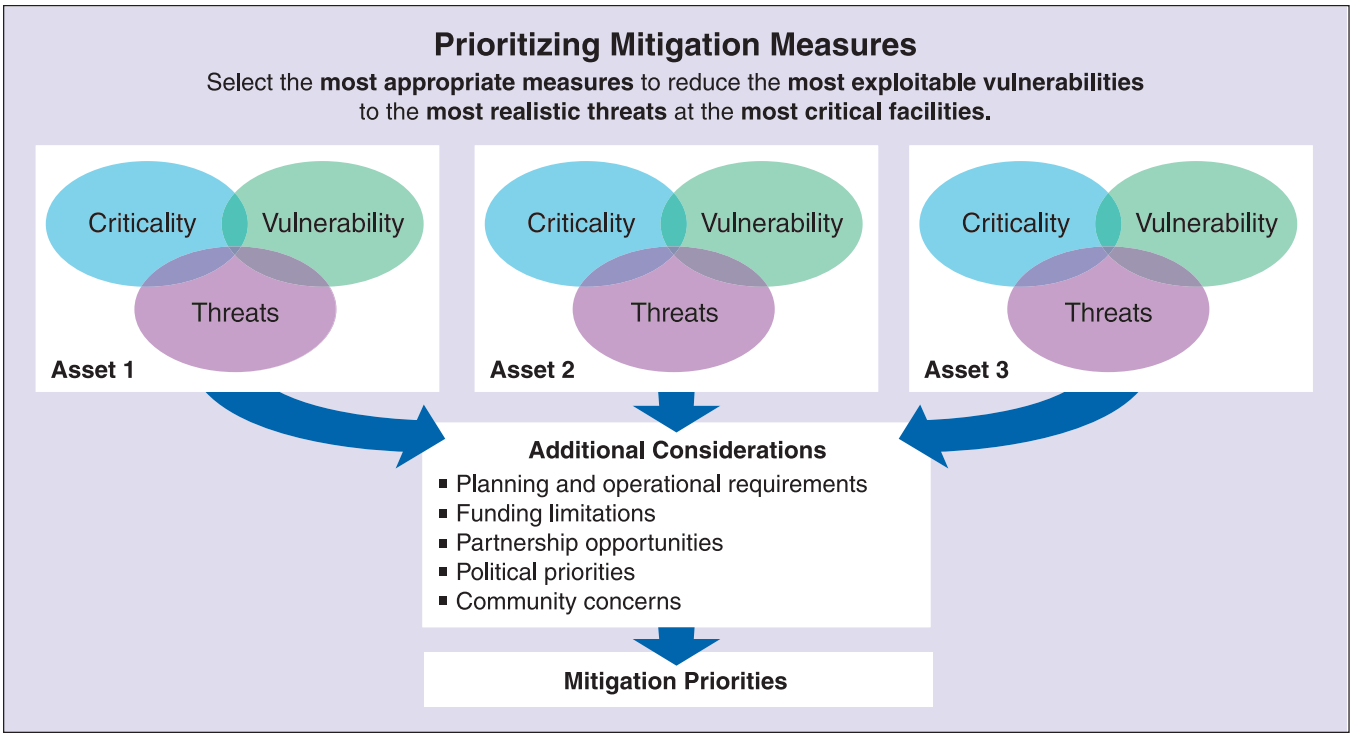
law enforcement agencies that can provide the planning team with a general characterization of terrorist and other such groups known to be active in your community, the tactics they may employ or have employed in the past, and projections of potential and emerging threats.

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 human-caused 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 human-caused 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 human-caused 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*