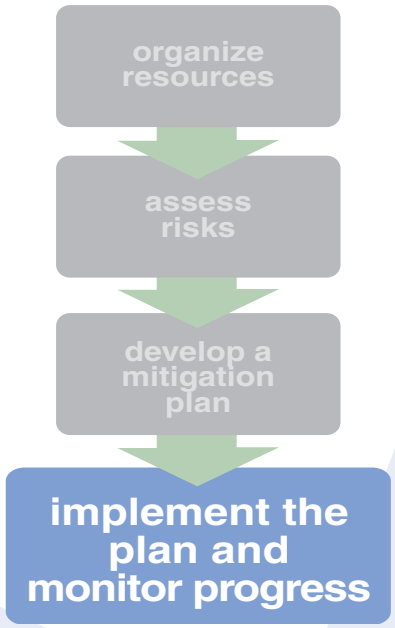
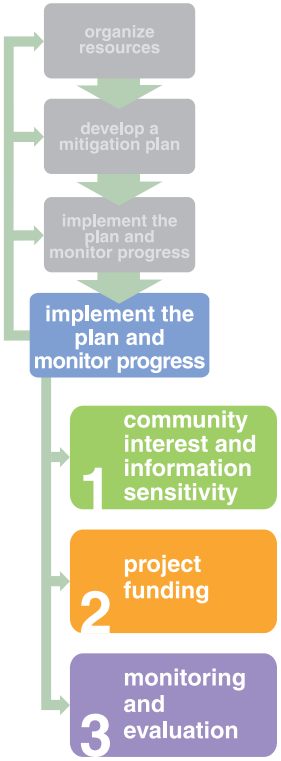
phase 4


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

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: Assuring the Success of the Hazard Mitigation Plan* (FEMA 386-4). This section will address special considerations for implementing mitigation measures unique to human-caused 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) measures. 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 measures 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 Human-Caused Hazard Mitigation Projects

At the time of this writing, there is little federal funding specifically earmarked for state and local use in mitigating against human-caused 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 measures 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 measures 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 human-caused 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 measures 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 human-caused disasters occurring in most communities (particularly in contrast to many naturally occurring events), the value and effectiveness of mitigation measures such as structural blast-resistance retrofits and land use regulations may never be realized. Other measures 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 measures, and the resulting inquiries and studies can provide valuable input into subsequent mitigation planning initiatives.

The monitoring and evaluation of the human-caused 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.